Imperial College London
Department of Computing

Cloud computing in the Large Scale Organisation
Potential benefits and overcoming barriers to deployment
V1.1

Martin Clifford Bellamy

February 2014

Supervised by Prof. John Darlington

Submitted in part fulfillment of the requirements for the degree of Doctor of Philosophy in Computing of Imperial College London and the Diploma of Imperial College London

Declaration

I hereby declare that, to the best of my knowledge, all material in this thesis which is not my own work has been properly acknowledged.

Martin Bellamy

Acknowledgements

First and foremost I would like to thank my supervisor, Professor John Darlington for his support and guidance. I would also like to thank Peter Pietzuch, and Brian Fuchs and Jeremy Cohen of the Imperial College Social Computing Group for their help over the course of my studies.

Thanks are also due to John Suffolk, who as the then UK Government CIO (2009) commissioned the G Cloud Phase 2 work [17], and to Denise McDonagh (G Cloud Programme Director), Andy Tait (G Cloud Deputy Programme Director) and to Andy Nelson the Senior Responsible Officer for the UK Government G Cloud programme for their support throughout. Significantly Bill McCluggage who was then deputy government CIO provided much stimulating input in the period 2009 to 2010.

Particular thanks are due to the volunteers who formed the G Cloud phase 2 team between Autumn 2009 and Spring 2010, notably the work strand leads and industry co leads, and also to John Fotheringham of Deloitte.

Finally, I would like to thank Michael Spurr, Chief Executive of the National Offender Management Service, who has continued to support my interest in Cloud computing since my transfer to NOMS in June 2010.

Copyright

The copyright of this thesis rests with the author and is made available under a Creative Commons Attribution Non-Commercial No Derivatives licence. Researchers are free to copy, distribute or transmit the thesis on the condition that they attribute it, that they do not use it for commercial purposes and that they do not alter, transform or build upon it. For any reuse or redistribution, researchers must make clear to others the licence terms of this work.

Abstract

There are three focal questions addressed in this thesis:

- Firstly whether large organisations, particularly public sector or governmental, can realise benefits by transitioning from the ICT delivery models prevalent in the late 2000s to use Cloud computing services?
- Secondly, in what circumstances can the benefits best be realised, and how and when can the associated risk reward trade-off be managed effectively?
- Thirdly, what steps can be taken to ensure maximum benefit is gained from using Cloud computing? This includes a consideration of the technical and organisational obstacles that need to be overcome to realise these benefits in large organisations.

The potential benefits for organisations using Cloud computing services include cost reductions, faster innovation, delivery of modern information based services that meet consumers' expectations, and improved choice and affordability of specialist services. There are many examples of successful Cloud computing deployments in large organisations that are saving time and money, although in larger organisations these are generally in areas that do not involve use of sensitive information.

Despite the benefits, by 2013 cloud computing services account for less than 5% most large organisations' ICT budgets. The key inhibitor to wider deployment is that use of Cloud computing services exposes organisations to new risks that can be costly to address.

However, the level of cost reduction that can be attained means that progressive deployment of Cloud computing services seems inevitable. The challenge therefore is how best to manage the associated risks in an effective and efficient manner.

This thesis considers the origin and benefits of Cloud computing, identifies the barriers to take up and explores how these can be overcome, and considers how cloud service brokerages can potentially develop further to close the gap by building new capabilities to accelerate take-up and benefits realisation. (292 words)

Table of Contents

PHD THESIS CLOUD COMPUTING IN THE LARGE SCALE ORGANISATION

POTENTIAL BENEFITS AND OVERCOMING BARRIERS TO DEPLOYMENT

PART 1: INTRODUCTION AND CONTEXT 10

1.0 CONTRIBUTION OF THIS PHD INCLUDING SUMMARY OF CONCLUSIONS 11
1.1 CONTEXT ,SCOPE OF WORK AND EXCLUSIONS. 11
1.2 CONTRIBUTION OF THIS PH.D. 12
1.3 WHY, DESPITE ATTRACTIVE BENEFITS, IS TAKE-UP OF CLOUD COMPUTING SERVICES RELATIVELY SLOW? 15
1.4 WHAT ARE THE MAIN BARRIERS THAT NEED TO BE OVERCOME? 17
1.5 HOW CAN LARGE ORGANISATIONS, FOR EXAMPLE UK GOVERNMENT, SYSTEMATICALLY ACHIEVE BENEFITS THROUGH OVERCOMING THE BARRIERS? 20
1.6 HOW CLOUD SERVICE BROKERAGES ARE LIKELY TO DEVELOP AND DRIVE TAKE-UP OF CLOUD COMPUTING S ERVICES, AND THE SERVICES SUCH BROKERAGE ORGANISATIONS WILL NEED TO OFFER? 20
1.7 NEXT STAGE OF RESEARCH NEEDED TO HELP ESTABLISH CLOUD SERVICE BROKERAGES. 21

2.0 MOTIVATION FOR THE PHD 23

3.0 HOW THE RESEARCH WAS DONE AND MY PERSONAL CONTRIBUTION. 25
3.1 INTRODUCTION 25
3.2 PERSONAL CONTRIBUTION 26

4.0 CONTEXT 28
4.1 HOW AND WHEN DID CLOUD COMPUTING ORIGINATE? 28
4.2 SO IS CLOUD COMPUTING JUST THE RETURN OF THE COMPUTER BUREAU USING INTERNET TECHNOLOGIES? IF NOT WHAT HAS CHANGED? 29
4.3 HOW CAN USING CLOUD COMPUTING SERVICES HELP BUSINESSES? 29
4.4 WHAT TYPES OF SERVICE ARE AVAILABLE? 30
4.5 CLOUD DEPLOYMENT MODELS 31
4.6 ICT AS A UTILITY 33
4.7 GETTING DATA IN AND OUT OF CLOUD SERVICES 34
4.8 CHALLENGES IN USING CLOUD COMPUTING SERVICES 35
4.9 CHAPTER CONCLUSION -- CLOUD COMPUTING IS BY NO MEANS A NEW CONCEPT 35

5.0 THE BENEFITS PROPOSITION 37
5.1 INTRODUCTION 37
5.2 POTENTIAL BENEFITS 37
5.3 FINANCIAL BENEFITS 39
5.4 THE BUSINESS REINVENTION POSSIBILITY 41
5.5 RISKS AND BENEFITS 44
5.6 CHAPTER CONCLUSION -- CLOUD COMPUTING HAS POTENTIAL TO BRING SUBSTANTIAL BENEFITS TO LARGE-SCALE ENTERPRISES THROUGH ECONOMIES OF SCALE/LOWER UNIT COSTS. 46

PART 2: IDENTIFICATION AND ANALYSIS OF FOUNDATION CAPABILITIES NEEDED FOR WIDESPREAD UTILISATION OF CLOUD COMPUTING SERVICES 48

6.0 FUTURE ICT OPERATING MODEL BASED ON UTILIZATION OF CLOUD-BASED SERVICES 50
6.1 CONTEXT FOR PUBLIC SECTOR ICT 50
6.2 IT IS CLOUD COMPUTING A FAD OR AN "INDUSTRY INFLECTION POINT"? 51

6.3 What is the likely timescale within which the switch to Cloud computing services will occur? 52
6.4 Defining characteristics of the expected "end state "model for government use of Cloud computing services 53
6.5 Survey of local authority ICT leaders expectations on cloud services adoption 56
6.6 Chapter conclusion -- UK Government is committed to a hybrid cloud 'cloud first' strategy 57

7.0 Technology – what's needed to deliver the cloud vision? 58
7.1 Synopsis and summary conclusions 58
7.2 Context and definitions 59
7.3 Standards 61
7.4 Technical architecture principles 62
7.5 Areas for further work by technical architecture work strand 64
7.6 Potential role for Services Orientated Architecture 66
7.7 Technical architecture risks 67
7.8 Chapter conclusion – large organisations will need to put in place a framework of standards and policies to ensure coherent and optimal use of Cloud computing services 68

8.0 Information Assurance considerations 69
8.1 Context 69
8.2 Key information assurance focus areas in a Cloud computing context 70
8.3 The criticality of "trust" 71
8.4 Desired information assurance outcomes 71
8.5 Information assurance objectives 72
8.6 How do Cloud computing information assurance risks arise – What are the points of vulnerability? 73
8.7 Mitigation of conventional information assurance risks 74
8.8 Mitigation of Cloud computing related information assurance risks 74
8.9 Information assurance related risks 75
8.10 Mitigating information assurance related risks 76
8.11 Organisational framework for achieving secure use of cloud services. 77
8.12 Strawman Information Risk Management Roadmap 78
8.13 Loss of service risks 79
8.14 Defence 'in depth' approach 79
8.15 Potential role of Cloud Services Brokers and Service Orientated Architecture 80
8.16 Rationalisation of government information assurance schema 81
8.17 Chapter conclusion – Managing the information assurance risks in using Cloud computing services 82

9.0 Service Management 84
9.1 Cloud computing ICT Service Management:- summary conclusions 85
9.2 ICT Service management challenges 88
9.3 Integrated service management model 89
9.4 Framework for ICT service management when using Cloud computing services. 90
9.5 Risks 91
9.6 A possible "end state "service management model for using Cloud computing services in the large-scale organisation. 92
9.7 A framework for cloud services integration. 93
9.8 Role of the cloud services broker. 93
9.9 Scope for a phased, multilevel approach to developing cloud service brokerages 96
9.10 Service Management roadmap for cloud services deployment. 98

9.11 CHAPTER CONCLUSION – MANAGING RISKS TO ICT SERVICE CONTINUITY WHEN USING CLOUD COMPUTING SERVICES 98

10.0 COMMERCIAL AND LEGAL IMPLICATIONS OF USING CLOUD COMPUTING SERVICES 101
10.1 INTRODUCTION: MARKET STRUCTURE FOR CLOUD COMPUTING SERVICES 101
10.2 OBJECTIVES FOR CLOUD COMPUTING COMMERCIAL FRAMEWORK 103
10.3 CORE COMMERCIAL PRINCIPLES FOR CLOUD COMPUTING SERVICES 103
10.4 ENSURING ONGOING COMPETITION IN THE MARKETPLACE FOR CLOUD COMPUTING SERVICES? 104
10.5 DEVELOPMENT OF THE MARKETPLACE FOR CLOUD COMPUTING SERVICES 106
10.6 DESIRED COMMERCIAL OUTCOMES 107
10.7 ACHIEVING TRANSITION 109
10.8 CHAPTER CONCLUSION -- THE MARKETPLACE FOR CLOUD COMPUTING SERVICES IS NOT PERFECTLY COMPETITIVE, WITH PROVIDERS DELIBERATELY AND EXTENSIVELY DIFFERENTIATING SERVICES 113

11.0 G CLOUD PHASE 2 PROPOSITION 114
11.1 INTRODUCTION 114
11.2 BARRIERS TO TAKE UP 114
11.3 USING CLOUD COMPUTING SERVICES TO IMPLEMENT BUSINESS PROCESSES 115
11.4 G CLOUD FOUNDING PRINCIPLES 117
11.5 G CLOUD BUSINESS CASE 120
11.6 CHAPTER CONCLUSION – THE G CLOUD BUSINESS CASE CONSERVATIVELY PROJECTED ICT COST REDUCTIONS IN THE REGION OF 15% TO 25% 124

PART 3: DELIVERY OF THE UK GOVERNMENT CLOUD COMPUTING STRATEGY IN THE PERIOD 2010 TO 2013; SUCCESSES, CHALLENGES AND PITFALLS. 126

12.0 OBSTACLES ENCOUNTERED IN IMPLEMENTING THE G CLOUD STRATEGY 129
12.1 CONTEXT: INCOMING GOVERNMENT'S POLICY OBJECTIVES 129
12.2 GOVERNMENT ICT SUPPLIER LANDSCAPE 130
12.3 THE G CLOUD STRATEGY WAS ADAPTED TO REFLECT THE POLICY OBJECTIVES OF THE INCOMING COALITION GOVERNMENT 136

13.0 UK GOVERNMENT CLOUD COMPUTING STRATEGY 137
13.1 ANNOUNCEMENT 138
13.2 SCOPE 138
13.3 SIMILARITIES BETWEEN THE PUBLISHED GOVERNMENT CLOUD COMPUTING STRATEGY AND THE G CLOUD PHASE 2 WORK OF 2009/10 140
13.4 IMPLICATIONS OF REVISED G CLOUD STRATEGY; CHANGES IN EMPHASIS FROM WORK DONE IN 2009/10 143
13.5 RISKS 145
13.6 COMPARISON WITH OTHER GOVERNMENTS' CLOUD COMPUTING STRATEGIES 146
13.7 CHAPTER CONCLUSION -- G CLOUD ANNOUNCEMENT 149

14.0 PROGRESS EIGHTEEN MONTHS AFTER PUBLISHING THE G CLOUD STRATEGY 153
14.1 SERVICES AVAILABLE ON G CLOUD 153
14.2 SUCCESSFUL DEPLOYMENT EXAMPLES 153
14.3 UNSUCCESSFUL ATTEMPTS TO USE G CLOUD SERVICES FOR MISSION-CRITICAL APPLICATIONS 160
14.4 PROCURING "MISSION CRITICAL" GOVERNMENT ICT IN 2012/13 164
14.5 HYBRID CLOUD PROPOSAL - PAN GOVERNMENT HOSTING FRAMEWORK 167
14.6 CHAPTER CONCLUSION 168

PART 4: CLOUD COMPUTING IN UK GOVERNMENT – OVERCOMING BARRIERS TO DEPLOYMENT AND NEXT STEPS 175

15.0 ASSESSMENT OF G CLOUD PROGRAMME TO DATE 176
15.1 CONTEXT 176
15.2 BARRIERS TO CLOUD COMPUTING DEPLOYMENT IN UK GOVERNMENT 176
15.3 AUTHORS PERSPECTIVE ON BARRIERS 179
15.4 CLOUD COMPUTING INDUSTRY DEVELOPMENTS 183
15.5 CHAPTER CONCLUSION -- THE UK GOVERNMENT IS ALREADY REALIZING SIGNIFICANT BENEFITS FROM USING CLOUD COMPUTING SERVICES; BENEFITS CAN BE ENHANCED THROUGH PERSISTING WITH EFFORTS TO UTILISE SHARED CLOUD SERVICES FOR CITIZEN FACING "LINE OF BUSINESS" PROCESSES. 183

16.0 CLOUD SERVICES BROKERAGE 186
16.1 CONTEXT 186
16.2 WHAT SERVICES WILL CLOUD SERVICES BROKERAGES NEEDS TO PROVIDE TO HELP THEIR CLIENTS OVERCOME BARRIERS TO DEPLOYMENT? 187
16.3 OPERATIONAL PROCESSES FOR CLOUD SERVICES BROKERS 200
16.4 CHAPTER CONCLUSION -- THERE IS A MARKET OPPORTUNITY FOR CLOUD SERVICES BROKERAGES; ESTABLISHING TRUST IS CRITICAL, AND ORGANISATIONS THAT INVEST IN BUILDING AUTOMATED CAPABILITIES WILL GAIN COMPETITIVE EDGE. 201

PART 5: KEY FINDINGS AND FURTHER RESEARCH AREAS 204

17.0 CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER WORK 205
17.1 CLOUD COMPUTING IS BY NO MEANS A NEW CONCEPT 205
17.2 BUT THE SIZE AND SCALE OF CLOUD COMPUTING PROVIDERS, AND THE LEVEL OF COST REDUCTIONS ACHIEVED, MEANS THE DELIVERY MODEL IS A "GAME CHANGER" 205
17.3 CONTINUED DEPLOYMENT OF CLOUD COMPUTING SERVICES SEEMS INEVITABLE 207
17.4 CLOUD COMPUTING HAS POTENTIAL TO BRING SUBSTANTIAL BENEFITS TO LARGE-SCALE ENTERPRISES THROUGH ECONOMIES OF SCALE/LOWER UNIT COSTS. 209
17.5 UK GOVERNMENT IS COMMITTED TO A HYBRID CLOUD 'CLOUD FIRST' STRATEGY 209
17.6 INITIAL DEPLOYMENTS WILL FOCUS ON RELATIVELY STRAIGHTFORWARD CASES, HOWEVER THESE WILL NOT HAVE A MAJOR IMPACT ON THE CORE OF ICT ACTIVITIES 210
17.7 USING COMMODITY CLOUD COMPUTING SERVICES FOR COMPLEX ORGANISATION SPECIFIC "LINE OF BUSINESS ACTIVITIES" IS DIFFICULT AND CHALLENGING 211
17.8 OTHER BARRIERS NEED TO BE ADDRESSED TO ACCELERATE BENEFITS REALISATION FROM CLOUD COMPUTING;- MANY OF THESE RELATE TO LEADERSHIP, CULTURE, CAPABILITIES AND PROCESSES 211
17.9 THERE IS A MARKET OPPORTUNITY FOR CLOUD SERVICE BROKERAGES; ORGANISATIONS THAT INVEST IN BUILDING AUTOMATED CAPABILITIES WILL GAIN COMPETITIVE EDGE. 212
17.10 SIGNIFICANT INVESTMENT IS NEEDED IN CLOUD SERVICE BROKERAGES TO DRIVE THE POTENTIAL OF CLOUD COMPUTING 213
17.11 AUTOMATION OF THE SERVICES TO BE PROVIDED BY CLOUD SERVICES BROKERS WILL YIELD FURTHER BENEFITS; HOWEVER THE STANDARDS TO DO THIS IN FULL ARE NOT YET AVAILABLE 215
17.12 A 'DEFENCE IN DEPTH' STRATEGY IS NEEDED TO MANAGE INFORMATION ASSURANCE CHALLENGES WHEN USING CLOUD COMPUTING SERVICES 216
17.13 A STRATEGIC APPROACH IS NEEDED FOR ICT SERVICE MANAGEMENT WHEN USING CLOUD COMPUTING SERVICES, WITH FOCUS ON HOW TO ENSURE SERVICE CONTINUITY AND ON PRESERVING DATA SHOULD A PROVIDER FAIL 217
17.14 THE MARKETPLACE FOR CLOUD COMPUTING SERVICES IS FAR FROM PERFECTLY COMPETITIVE, WITH PROVIDERS DELIBERATELY AND EXTENSIVELY DIFFERENTIATING SERVICES 219
17.15 ORGANISATIONS WILL NEED TO ACCEPT, AND EFFECTIVELY MANAGE NEW TYPES OF RISK,

TO SUCCEED WITH THE USE OF CLOUD COMPUTING SERVICES 219
17.16 THE UK PUBLIC SECTOR IS GAINING VALUABLE EXPERIENCE FROM THE GROWING SUCCESS OF CLOUDSTORE 221
17.17 THE "CHANGE JOURNEY" FOR DEPLOYING CLOUD COMPUTING SERVICES WILL TAKE PLACE OVER A DECADE OR MORE, AND INVOLVES A MULTILEVEL TRANSFORMATION OF THE SUPPLIER AND CONSUMER MARKETPLACES, AFFECTING PEOPLE, PROCESS AND TECHNOLOGY 221
17.18 THE BROADLY BASED VOLUNTEER APPROACH TO THIS RESEARCH HAS YIELDED INPUT FROM A WIDE VARIETY OF PERSPECTIVES; -THIS APPROACH SHOULD BE CONSIDERED IN SIMILAR CASES MOVING FORWARDS. 222

18.0 RECOMMENDATIONS FOR FURTHER WORK 223
18.1 TO CONSIDER THE ORGANISATIONAL MODELS AND GOVERNANCE STRUCTURES THAT WILL ACCELERATE REALISATION OF THE BENEFITS OF CLOUD COMPUTING 223
18.2 TO IDENTIFY HOW BEST TO ENSURE INFORMATION ASSURANCE FOR ORGANISATIONS MAKING USE OF CLOUD SERVICES 223
18.3 TO DEVELOP A POSITIVE PROPOSITION FOR ICT SPECIALISTS, AND A ROADMAP THAT WILL ENABLE EXISTING PRACTITIONERS TO LEAD THE WAY IN THE TRANSITION TO CLOUD COMPUTING SERVICES 223
18.4 TO ESTABLISH HOW TRUSTED CLOUD SERVICE BROKERAGES CAN BEST BE ESTABLISHED. 224
18.5 TO DETERMINE HOW BEST TO AGREE THE TECHNICAL STANDARDS THAT ARE NEEDED FOR FULL REALISATION OF THE POTENTIAL BENEFITS OF CLOUD COMPUTING 224

COMPETING INTERESTS 225

AUTHORS CONTRIBUTION 225

BIBLIOGRAPHY 226

ANNEX 1: PAPER AND SLIDES PRESENTED ON 27 JUNE 2013 TO IEEE 2013 INTERNATIONAL WORKSHOP ON SERVICES DISCOVERY AND COMPOSITION 220

List of tables

Table 1: Market structure (reproduced from "Economics" [92] by Begg, Fischer and Dornbusch)

Table 2: G Cloud Authority: potential for delivering benefits and addressing obstacles to Cloud computing deployment

Table 3: Potential cost savings attainable if UK central government adopts cloud computing

Table 4: Low average system utilisation results from a project initiated approach to provisioning data centre based systems

Table 5: Repositioning of G Cloud strategy following 2010 general election

Table 6: Implemented G Cloud strategy: potential for delivering benefits and addressing general obstacles to Cloud computing deployment

Table 7: Assessment or fit of public cloud services for "stand-alone" deployments that do involve use of sensitive data.: potential for delivering benefits and addressing obstacles to Cloud computing deployment

Table 8: Implemented G Cloud strategy: potential for delivering benefits and addressing obstacles to Cloud computing deployment for moderate complexity 'end user' services
Table 9: Implemented G Cloud strategy: potential for delivering benefits and addressing obstacles to Cloud computing deployment for high complexity/sensitivity 'end user' services
Table 10: Implemented G Cloud strategy: potential for delivering benefits and addressing obstacles to Cloud computing deployment for MoJ wide ICT services
Table 11: Pan government hybrid cloud proposal: potential for delivering benefits and addressing obstacles to Cloud computing deployment for high complexity/sensitivity 'end user' service
Table 12: Consolidated assessments of ability of cloud usage scenarios to deliver benefits and overcome obstacles
Table 13: Ranked fit of deployment scenarios to benefits and obstacles
Table 14: Ranking of obstacles to cloud deployment
Table 15: 2013 outturn on risks envisaged by G Cloud programme team in 2010
Table 16: 2013 outturn on risks envisaged in published G Cloud strategy (2011)
Table 17: Brokerage services to address obstacles to Cloud computing deployment

List of figures

Figure 1: NIST Cloud computing definition (diagrammatic representation)
Figure 2: Cloud computing service layers (IaaS, PaaS, IaaS)
Figure 3: Interfaces requires to automate the selection and deployment of Cloud computing services.
Figure 4: Depiction of "defence in depth" approach for cloud services information assurance.
Figure 5: Cloud computing service management roles.
Figure 6: Relationship between complexity of cloud services and intensity of service management engagement
Figure 7: Ranking of Cloud computing deployment options
Figure 8: Cloud Services Brokerages – Potential Services
Figure 9: Model for using insecure Cloud computing services to underpin secure business processes

Categories and subject descriptors
Computer and information science, computer communication networks, software engineering

General terms
Management, performance, economics, reliability

Keywords
Cloud computing, distributed systems, service orientated architecture

PhD Thesis Cloud computing in the Large Scale Organisation

Potential benefits and overcoming barriers to deployment

Part 1: Introduction and context

Chapters 1 to 3 sets out the background to the Ph.D. and the contribution made. Chapters 4 and 5 explain the origins of Cloud computing, and how the combination of scale, location, standardisation, automation and self provisioning that are together termed “industrialisation” yield a substantial level of cost reduction over the majority of today’s commercial data centres.

Academic studies have set out the potential for cost savings of 65%-85% on data centre and applications costs [2,3], and this is consistent with the author’s previous experience at Reuters, where largely as a result of the adoption of the core principles of Cloud computing, certain large scale ICT costs in the early 2000s were similar to the unit cost levels achieved by today’s large-scale Cloud computing providers.

The level of cost savings attainable seems to indicate that progressive migration of the ICT services used by businesses to the Cloud computing model is inevitable.

1.0 Contribution of this PhD including summary of conclusions

1.1 Context ,scope of work and exclusions.

Compared to conventional approaches of providing computing services, the industrial scale and high utilisation levels achieved by Cloud computing providers enables data centre and application costs to be reduced by up to 65-85% [2,3]. This level of cost reduction together with the other benefits that can be achieved mean that it seems inevitable that organisations will make growing use of Cloud computing services over time. Indeed, there is likely to come a time when the advantages organisations accrue through using Cloud computing services will make their deployment in some industries and business sectors a “competitive necessity”, with organisations that have failed to make the transition no longer able to compete effectively in their marketplaces. However, in most large organisations the use of Cloud computing is currently limited to a minority of possible deployment opportunities, typically those that do not involve business critical services or sensitive data.

The work undertaken as part of this Ph.D. has focused on the use of information and communications technology (ICT) to underpin the internal and customer facing business processes of large governmental organisations. Such business processes typically support transactions (e.g. apply for a driving licence, make a payment of jobseekers allowance) and information services (e.g. provide a forecast of the state pension entitlement I am likely to receive). In most governmental organisations the ICT to underpin such business processes accounts for a substantial majority of ICT spend. This is due both to the number and complexity of the business processes involved, and to the large number of citizens who need to be served (which can be up to 60,000,000 in the UK). There are significant security requirements to maintain the confidentiality, integrity and availability of the datasets needed to provide such services.

Excluded from the work done within the Ph.D. are data sets that have the very highest security levels (e.g. military and diplomatic information and other datasets classified as secret or top-secret), and also use of ICT for specialist purposes such as control systems, multimedia processing, gaming etc.

1.2 Contribution of this Ph.D.

The main contribution of this PhD is an analysis of the factors inhibiting or preventing widespread adoption of Cloud computing facilities in large governmental organisations, and an elicitation of the means by which these factors could be overcome. This analysis leads to the identification of the opportunity for the emergence of Cloud computing services brokerages, and the definition of the various roles such organisations will need to fulfill.

The generic factor inhibiting wider deployment is that use of Cloud computing services exposes organisations to new risks. While the inherent risks can be managed, in the near term significant investment in skills, processes, tools and technology is a prerequisite for doing so efficiently. For most organisations that use ICT services, the level of investment needed will often be prohibitive.

Cloud service brokerages are needed to assist organisations that make intensive use of ICT in overcoming the multi-dimensional and complex barriers that would otherwise inhibit the transition of core business services to Cloud computing services, and thus delay realisation of the potential benefits.

Cloud brokerage services can share costs across organisations, investing strategically to assist organisations with the use of Cloud computing services and management of the associated risks, developing service portfolios that reduce upfront costs, so that use of Cloud computing services becomes the best choice on a project by project basis.

The thesis critically examines the work done during Phase 2 of the UK Government Cloud computing programme, including its proposal that an internal cloud service brokerage (the “G Cloud Authority”) is established to assist in mediating between Cloud computing providers, and users of ICT services.

The main conclusions (summarised in this chapter and elaborated in Chapter 17) are:

- Cloud computing is by no means a new concept (17.1)

- The size and scale of Cloud computing providers, and the level of cost reductions the deployment model can achieve, means the delivery model is a “game changer” (17.2)

- Continued deployment of Cloud computing services is seemingly inevitable (17.3)

- Cloud computing has potential to bring substantial benefits to large-scale organisations through economies of scale/lower unit costs. (17.4)

- UK Government is committed to a hybrid cloud 'cloud first' strategy, the G Cloud (17.5)

- Initial deployments of the G Cloud will focus on relatively straightforward cases, however these will not have a major impact on the core of ICT activities (17.6)

- Using commodity Cloud computing services for business critical organisation specific' "line of business activities" is difficult and challenging (17.7)

- Other barriers need to be addressed to accelerate benefits realisation from Cloud computing;- many of these relate to "soft factors" such as leadership, culture, capabilities and processes (17.8)

- There is a market opportunity for cloud service brokerages; organisations that invest in building automated capabilities will gain competitive edge. (17.9)

- Significant investment is needed in cloud service brokerages to drive the potential of Cloud computing (17.10)

- Automation of the services to be provided by cloud services brokers will yield further benefits; however the standards to do this in full are not yet available (17.11)

- A 'defence in depth' strategy is needed to manage Information Assurance challenges when using Cloud computing services (17.12)

- A strategic approach is needed for ICT service management when using Cloud computing services, with focus on how to ensure service continuity and preserve data should a provider fail (17.13)

- The marketplace for Cloud computing services is not perfectly competitive, with providers deliberately and extensively differentiating services (17.14)

- Organisations will need to accept, and effectively manage new types of risk, to succeed with the use of Cloud computing services (17.15)

- The UK public sector is gaining valuable experience from the growing success of its online catalogue for the selection and purchase of Cloud computing services, the CloudStore (17.16)

- The “change journey” for deploying Cloud computing services will take place over a decade or more, and involves a multilevel transformation of the supplier and consumer marketplaces, affecting people, process and technology (17.17)

- The broadly based volunteer approach to this research has yielded input from a wide variety of perspectives;- this approach should be considered in similar cases moving forwards. (17.18)

The scope for further work is elaborated in Chapter 18, with the priority areas comprising:

- Consideration of the organisational models and governance structures that will accelerate realisation of the benefits of Cloud computing (18.1)

- Identification of how best to ensure information assurance for organisations making use of cloud services (18.2)

- Development of a positive proposition for ICT specialists, and a roadmap that will enable existing practitioners to lead the way in the transition to Cloud computing services (18.3)

- Assessment of how trusted cloud service brokerages can best be established (18.4)

- Determination of how best to agree the technical standards that are needed for full realisation of the potential benefits of Cloud computing (18.5)

This thesis contributes through building understanding and proposed solutions in the following areas:

I. Why, despite attractive benefits, is take-up of Cloud computing services relatively slow?

II. What are the main barriers that need to be overcome?

III. How can large organisations, for example UK government, overcome the barriers to systematically achieve benefits?

IV. Why will the cost of overcoming barriers to Cloud computing take-up remain prohibitive for many organisations?

V. How cloud service brokerages are likely to develop and drive take-up of Cloud computing services, and what are the services such brokerage organisations will need to offer?

VI. The next stages of research needed to help establish cloud service brokerages.

1.3 Why, despite attractive benefits, is take-up of Cloud computing services relatively slow?

Organisations can potentially benefit substantially from using Cloud computing services both to address new ICT related needs, and to replace conventional 'on premise' systems. In addition to cost reduction, the benefits can include faster delivery of the ICT needed for business innovation, and creating business platforms with the quality of user interfaces needed to meet consumers' expectations for services in the Internet age. As modern economies see greater development of "networked organisations", Cloud computing can provide a safe environment for collaboration and shared processes. What is also clear is that the full transition from conventional ICT to cloud will take time, and that with current approaches in many organisations the transition will take place over a period of more than a decade.

Cloud computing is proven to be a viable delivery model [62] for many of the information services used by consumers and businesses, and in certain contexts has clear advantages over conventional approaches:

- Enabled by Internet standards and widespread availability of broadband networking

services, the large consumer focused Internet firms have shown that the Cloud computing model can successfully deliver affordable, quality information services to hundreds of millions of users. The centralised nature of Cloud computing services brings other advantages too; information can be appropriately shared between different users, for example with e-mail or social networking. Additionally the model is well-suited to underpin the delivery of services to mobile devices, the use of which has grown rapidly over recent years.

- The availability on tap of as much or as little resource as is needed, removing the expense of purchasing and maintaining dedicated hardware, reduces upfront risk for organisations that are introducing new information-based services.
- Likewise, organisations such as Microsoft, Google, Amazon Web Services, and salesforce.com have shown that the same model can be viable for the delivery of information services to businesses, and that in certain contexts this offers real benefits over conventional approaches. The benefits can include much improved "consumer quality" user interfaces, enhanced functions such as collaboration and desktop videoconferencing, access to social networking services integrated at the contact centre and rapid scaling up and down of infrastructure capacity. In certain contexts, these services are enabling businesses to realise substantial value including more efficient operations and faster innovation.
- The Cloud computing model also lowers costs of sale and market entry costs for new ICT providers, and as a result is helping enhance the dynamism of the ICT services marketplace. For example SMEs and other new entrants are now successfully using the Cloud computing model to sell ICT services to large organisations including the UK government.
- The increasing diversity of sources of supply, and the pay per use model, enable specialist needs to be met affordably, including cases such as the creation of a dedicated in-house solution for a small number of users where previously costs would often have been prohibitive.
- The Cloud computing approach is also proven to add value at the community level. Organisations such as Visa, MasterCard, VocaLink, and airline booking organisations have for many years offered services (for business communities) where data is legitimately shared between individuals and organisations with a common interest. Cloud computing has enabled new community applications to develop, the most prevalent of which is social networking.
- Cloud computing continues to have considerable market momentum, with substantial

business interest in using commodity services such as development/test, and common services such as HR and finance applications.

Most large organisations are already making some use of Cloud computing services, typically on a self-contained or stand-alone basis, where there are readily attainable benefits and relatively small deployment overheads, however

- the scope for such self-contained deployments represents only a relatively small proportion of current ICT costs,
- the majority of ICT spend in many organisations is to underpin specific "line of business" processes that create "unique business value add". Using Cloud computing services in these cases has the potential to deliver substantial benefits but is much more challenging to achieve. This is because there are significant risks that need to be managed. On a project by project basis, the cost and time required to overcome such risks is typically prohibitive, resulting in continued use of conventional approaches,
- systematic use of Cloud computing services requires new skills. Presently such capabilities are complex and time-consuming to build internally, and potentially hard to source externally, although there are a growing number of "cloud service brokerages" addressing these areas.

Organisation specific "line of business" processes can be replicated using Cloud computing services, although it is usually necessary to use a combination of internal and external services to do so. In such cases the services used will typically include some existing publicly available services, and some new ones that address the genuinely unique element of the business problem. The services need to be integrated with each other, and with sensitive organisational data. While there are some exemplars such as Japan Post [16], organisations are finding that, on a project by project basis, the time and cost to overcome the various barriers is prohibitive, resulting in continued use of conventional approaches.

1.4 What are the main barriers that need to be overcome?

Cloud computing thus introduces significant new risks [8] as it involves placing organisational information into shared resources that are managed and controlled by third parties. Threats can thus arise from Cloud computing suppliers, from other users of the Cloud computing service, as well as from third parties illicitly obtaining access via the Internet, circumventing access controls

and protection. Additionally there may be legal risks (arising from breach of data privacy or location rules), and risks that result from unintended aggregation of services.

Cloud computing has not become the default approach for new ICT investment within businesses. This is because there are risks, gaps and barriers that inhibit use for organisation specific business processes, and while many of the issues can in theory be overcome, doing so is often costly and complex to achieve. In particular there remain significant risks in attempting to use Cloud computing services to implement the "business critical" processes that underpin organisations' unique purposes. Most large organisations have established a unique "enterprise architecture" of databases and transactional systems. Such services are challenging to implement using Cloud computing services, which by definition provide identical commodity services to very large user communities. Concerns in using Cloud computing services include:

- Security, which is the top risk cited by businesses. As explained earlier, using public Cloud computing services involves trusting third parties with organisational and/or personal information that is held in a shared environment. There are at least 30 potential risk areas, and some of the technologies and many of the processes involved are still to reach maturity. Hence even where cloud providers' intentions are sound, there is a risk that providers may not have the capabilities needed (technical or procedural) to ensure that information is protected, that availability is assured, and that compliance with legal requirements will be maintained.
- Where it is necessary to integrate more than one cloud service to generate a unique business process, the selection and integration of services is complex due to the different standards (technology, data, service, security) used by suppliers. Providers may not publicly disclose all the characteristics of their services, creating an "information asymmetry" that can further add to risk.
- "Power imbalance" between Cloud computing providers and consumer, resulting from the large scale of many cloud providers, with the impact intensified by the prevalence of automated low-cost sales and support models. Businesses using cloud services have reported that it becomes difficult to obtain information or help during periods when service problems are being experienced; and if this results in a business critical process not being available this can result in serious risk to the consuming organisation.
- Legal compliance also presents a challenge, for example as data protection legislation may restrict the ability to hold data on citizens outside their home country. Public Cloud computing services providers do not always disclose when data is stored outside the home country. Ensuring compliance can become complicated, with different handling

policies potentially applying to different categories of data, for example user data, authentication data, and management information. Further, there may be different interpretations for “data at rest”, and “data in flight”.

While in theory the above risks can be managed, there are gaps and shortfalls in some current ICT methodologies which increase the risks from the perspective of cloud consumers. For example there are not recognised approaches for developing a Cloud computing strategy, building the appropriate portfolio of internal skills, developing business cases, designing business processes using cloud services, testing across a combination of services or for ongoing service management.

Hence there are complex legal, security, service, technical, commercial and business continuity issues to overcome in using Cloud computing services. It is easier to address these barriers for relatively self-contained deployments that are handling less sensitive information, and consequently this is where large organisations have tended to begin using Cloud computing services. Some small organisations and many start-ups are making much more extensive use of Cloud computing services [64]; this enables a wide range of services to be acquired for minimal capital outlay. Within start-ups in particular, there is often greater openness to new ways of working, and greater tolerance of risk.

Compared to other professions, ICT is arguably immature in its methodologies and has not been able to consistently reuse existing assets. This results in low levels of asset reuse, and thus a high level of “reinventing the wheel”. Enterprise architecture and governance initiatives to achieve reuse have been slow to gain traction. Larger organisations seeking to use Cloud computing services for core business activities need to demonstrate that they have the ability to manage the associated risks;- the most practical way of doing so may be by engaging a specialist cloud services broker.

While UK Government is promoting the use of Cloud computing services, it is recognised that today’s public cloud services cannot meet all needs for example because information security concerns inhibit the business appetite for accepting dependencies for critical services that are outside UK jurisdiction. Another challenge is that much ICT in government (and most large private sector) organisations depends on “legacy” applications that have been created over the last 30 years or more, and which do not comply with the “Internet” standards on which cloud services are based.

1.5 How can large organisations, for example UK government, systematically achieve benefits through overcoming the barriers?

A more strategic approach is thus needed, and the principles of Service Orientated Architecture (SoA) are highly relevant. Combinations of SoA services hosted on Cloud computing platforms can potentially be used (and reused) to create complex line of business processes, sourcing "best in-class" services for generic process elements, creating bespoke business logic only where absolutely essential.

Again, doing this successfully requires a different set of ICT skills, attitudes and behaviours from those needed to deliver conventional "on premise" ICT solutions.

While over time, these skills can be built within an organisation; in the short term many established ICT departments will find doing so challenging.

1.6 How cloud service brokerages are likely to develop and drive take-up of Cloud computing services, and the services such brokerage organisations will need to offer?

Organisations will thus be attracted by propositions which can deliver the cost reduction and other benefits of Cloud computing in a way which reduces upfront costs and mitigates risks. Cloud services brokers can assist with the design of Cloud computing based solutions, and with the creation of business cases showing how such approaches can reduce costs, accelerate delivery times, and mitigate risks.

There is therefore a market opportunity for the emerging category of ICT services organisation (that has been termed 'cloud services brokerage') to assist potential consumers of Cloud computing services in selecting and integrating services and managing relationships with providers. There is scope for cloud service brokerages to build the capabilities to reduce the costs of building business processes, and to deliver these more effectively and in shorter timescales. The types of service that cloud services brokerages could provide are described in chapter 16 of this thesis; for example they may include: –

- Describing Cloud computing services, both functional and non-functional aspects
- Selecting suitable providers, and managing relationships
- Specifying interfaces, to allow purchase, provisioning, billing, service management, and

security management of Cloud computing services, as well as accessing the core functionality

- Creating a framework for efficient creation of organisation specific processes, created from a composition of cloud services
- Implementing integrated toolsets for ongoing management and monitoring of cloud-based business processes
- Handling the administration, including billing and obtaining "service credits" where applicable
- Maintaining ongoing oversight of the cloud services marketplace, initiating "switching" on clients' behalf to the best cloud services to meet their needs. This requires the cloud services broker to have the ability to migrate data between service providers, and potentially to maintain a copy of data to assist with recovery should a provider fail

Achieving the above require cloud service brokerages to invest up front in areas such as selection and relationship building with cloud service providers, comprehensive provider due diligence, building know-how and insight into Cloud computing services and their future evolution, developing design patterns that provide their clients with resilience and avoid lock in, negotiating preferential commercial terms with cloud providers, and creating tools for data migration, service management etc.

While consuming organisations, assuming sufficiently strong levels of focus and commitment, could invest internally to overcome the challenges in using Cloud computing services, the overheads of doing so are substantial. As ICT investment is usually triggered by a business need that needs to be resolved within a defined timescale, on an ongoing "case-by-case" basis, organisations usually find it more practical to continue with conventional approaches to building ICT solutions.

1.7 Next stage of research needed to help establish cloud service brokerages.

Cloud service brokerages have already begun to develop, but today tend to support deployment of generic Cloud computing services to meet recurring needs such as e-mail and office software provision etc., rather than the creation of "line of business" processes using a combination of cloud services.

For most organisations offering cloud brokerage services, it is generally the case that the

"upfront" investment in building the necessary capabilities is limited. As a result today's cloud brokerage services are often heavily dependent on skilled (and therefore costly) expertise. Analogous to the upfront investment put into for example semiconductor fabrication plants, there is scope for investment in tooling for cloud service brokerages to and lower the unit costs of delivering relevant services.

However, a stronger business case is needed for cloud service brokerages to justify upfront investment in the toolsets and capabilities needed to deliver the above services efficiently. It is critical that cloud services brokers are trusted to act in organisations' or consumers' interests. Potentially these issues could be addressed, and the market could thus be catalysed by business communities or trade associations 'franchising' a small number of brokerage organisations (typically one or two) with the mandate to provide cloud service brokerages for their industries. Potentially the case for investment could be enhanced by the sponsorship of some new cross sector business services that will provide the broker with an initial revenue stream, and which will subsequently support the extension of a common cloud services model across member organisations.

Further research is needed to identify

- the range of services needed from cloud service brokerages, and to identify the range of attributes (hard and soft) both the brokerages, and the cloud services that they help deploy, will need to demonstrate.
- the scope for automation within cloud service brokerages to reduce costs of selection, integration, deployment, management and commercial and related overheads, as it will be through such automation and consolidation of expertise that brokerages build their competitive advantage.
- How cloud service brokerages can achieve market differentiation through focusing on a particular sector or geography. This will enable "in-depth" know-how to be built of business needs and of relevant services, thus enhancing competitive edge.

2.0 Motivation for the PhD

This Ph.D. arose as a result of a speculative e-mail I sent in summer 2009 to Prof John Darlington at Imperial College, London. At the time, I had just been invited to take a secondment into the UK Government's Cabinet Office to lead the initial work on the UK Government's Cloud computing programme. This initiative, to be known as the G Cloud Programme, was clearly going to be a substantial undertaking with the potential to drive change in the technology, the operational processes and above all the ways of working that underpin government ICT.

At the time, I had spent the best part of 30 years working in ICT following a computer science degree at Imperial College, London. After Imperial I had worked initially for BT as a product manager, then for over 13 years at Reuters in a variety of marketing and technology roles, followed by spells in consultancy, academia and since 2003 as an agency CIO role in the UK public sector. My career at the time had encompassed using ICT to solve business challenges; during the period I had encountered many similar challenges, but had found it difficult to reuse existing ICT investments even where it seemed that the fundamental business issue being addressed was near identical to one that had been resolved elsewhere. Some of my roles had involved attempts at "reuse"; however experience had shown that inheriting and reusing high-performance IT systems was extremely complex, and that it was typically easier to start again even though in theory there were many common services that could have been redeployed.

The barriers to reuse, coupled with a business environment where there are incentives for ICT suppliers to "provide a brand-new solution, that is innovative, effective and which uses the very latest technology" have tended to mean that in most enterprises, including government, reuse has happened far less frequently than could have been the case. While from the perspective of a specific business problem a bespoke ICT solution will often be the quickest and therefore preferred route to the goal, over time when looked at in the broader perspective, a series of bespoke solutions creates an ever harder to manage "spaghetti" which then inevitably delays the pace of innovation and change.

Many 'enterprise architecture' initiatives have attempted to mitigate this problem; introducing approaches such as corporate data models, preferred vendors, technical policies etc that have had the common goal of achieving convergence of ICT infrastructure and standards. While many of these initiatives have achieved progress, their overall impact has been significantly inhibited by the dynamic nature of ICT; innovation is happening all the time, suppliers create new versions

of existing software products and new types of hardware (for example mobile devices) become available. Innovation has often happened in multiple “parallel streams”, in many cases in areas where standards have not yet been defined. The net result is that most organisations have “families” of technologies and standards; i.e. areas of ICT conceived at different times with significant compatibility between some services, but still with boundaries that inhibit the ready flow of information between business processes, applications, databases and networks.

When I began work on this Ph.D. in 2009, public Cloud computing services such as Amazon EC2 [51], salesforce.com [16] and Google apps [15] had taken off and were rapidly gaining market share. Some public cloud providers were known to have invested in large-scale standardized virtualized automated data centres that had achieved substantial reductions in unit costs. It was clear that emerging possibilities included both using public cloud services to address new business requirements, and/or adopting a “private cloud” approach, replicating the engineering principles adopted by the cloud providers to streamline and reduce the cost of current ICT infrastructure. It was also clear that the full transition to cloud will take place over a period of a decade or more, and that there is a related opportunity for data centre rationalisation and consolidation initiatives to drive down legacy costs during the transition period.

These opportunities are recognised in the UK government ICT strategy that was published in 2011. This commits central government to a target of 50% of new business initiatives to be delivered using public cloud services by 2015. This seemed to be a substantial real-world example that merited study.

3.0 How the research was done and my personal contribution.

As set out in the summary, there are three focal questions addressed in this thesis:

- Firstly whether large organisations, particularly public sector or governmental, can realise benefits by transitioning from the ICT delivery models prevalent in the late 2000s to use Cloud computing services?,
- Secondly, in what circumstances can the benefits best be realised, and how and when can the associated risk reward trade-off be managed effectively?,
- Thirdly, what steps can be taken to ensure maximum benefit is gained from using Cloud computing? This includes a consideration of the obstacles, both technical and organisational, that need to be overcome to realise these benefits in large organisations.

3.1 Introduction

The research for this Ph.D. has been undertaken as part of my role as a civil servant, including my secondment into the Cabinet Office in 2009 as G Cloud Programme Director. The PhD also incorporates research initiated within the scope of my role of Change and Information and Communications Technology Director (CICT Director) at the National Offender Management Service in the period June 2010 to June 2013.

In summer 2009, I invited volunteers from the ICT industry and government departments to join a collaborative research exercise to define the strategy for use of Cloud computing services in government. Over 100 individuals volunteered to join the G Cloud Programme team.

The formation of the multi-organisation, volunteer-based G Cloud programme team provided a broadly based research capability that operated from October 2009 through to April 2010. It proved to be an effective research model, and this approach resulted in a holistic proposal for using Cloud computing services in government. Much of this work is also applicable to other large multi-divisional organisations.

3.2 Personal contribution

The personal contribution that is reported in this thesis comprises firstly the synthesis of all of the various inputs described and deriving general principles and procedures applicable to the adoption of Cloud computing in large organisations. Secondly, as described in parts three and four, from practical experience of deploying Cloud computing services I have derived conclusions on the obstacles that need to be overcome for successful widespread deployment, and the approaches for doing so.

My personal contribution between September 2009 and May 2010 was as programme director, leading and directing the initial research exercise that took place. I did this initially by forming a programme board consisting of the senior public sector volunteers. At the second meeting of this group I proposed and built support for the research to be undertaken through eight work strands that were to be overseen by the programme board, that I chaired. My role comprised directing the research programme including providing overall leadership for all workstrands, reviewing their outputs (including chairing joint reviews at the programme board), and moderating/directing the outcomes of workstrands to ensure an overall integrated and viable concept for moving forwards.

Once all the work strand reports were complete in April 2010 I led the process of deriving the “G Cloud Founding Principles” which were documented in a separate report [54].

In Spring 2010 I moved from the Cabinet Office into my present role of Change and ICT Director at the National Offender Management Service. Since then I have personally led opportunities to utilise Cloud computing services to deliver business requirements, and have thus assessed both successful and unsuccessful deployment examples at considered later in this thesis. I have retained an involvement with the G Cloud programme through continued membership of the G Cloud Delivery Board.

I have also commissioned analysis of existing public-sector deployments of Cloud computing services across organisations such as Ordnance Survey, Warwickshire and Hillingdon Councils, and the Government Digital Service. This research is documented in an internal report titled “Cloud Deployments Review” that was issued in May 2012 [57]. This thesis includes a summary of that research.

The above research has been complemented by reviews of applicable literature, speaking at conferences, visits to suppliers and establishing contact with representatives of other governments who are active in the Cloud computing area. This work has included submitting a paper based on the thesis to an academic conference, the IEEE 2013 Services Congress that took place in Santa Clara California in June/July 2013. The paper is titled "Adoption of Cloud Computing Services by Public Sector Organisations", and was accepted following a peer review process. This, and the supporting slides presented on 27th June 2013 at the IEEE 2013 International Workshop on Services Discovery and Composition (SDC 2013) are attached at Appendix 1.

The work strands and the title of their reports are:

- Service specification – G Cloud vision
- Technical architecture – Technical architecture workstrand report
- Service management – Service management, organisation and governance approach
- Information assurance – Information assurance workstream report: strategy for the high-level design
- Commercial architecture – Commercial strategy team work stream report
- Business case – G Cloud programme strategic outline case

Additionally I sponsored a "quick wins" work strand tasked with getting into place some live demonstrations and prototypes, and an overall "programme management" work strand that provided the Programme Management Office function to develop the overall plan, drive implementation, and ensure the expected deliverables were produced to agreed time and quality standards.

Part this thesis is based on the reports referenced above which were published on the Cabinet Office website in 2011 [19, 23, 25, 26, 27, 47, 51, 54].

4.0 Context

4.1 How and when did Cloud computing originate?

> " If computers of the kind I have advocated become the computers of the future, then computing may someday be organised as a public utility just as the telephone system is a public utility... The computer utility could become the basis of a new and important industry."
>
> —John McCarthy, speaking at the MIT Centennial in 1961[2]

As the above quotation from John McCarthy illustrates, Cloud (or utility) computing is by no means a new concept. Indeed in the 1960s computers were extremely expensive to purchase, and many organisations sourced their computing services from a "pseudo-cloud" provider i.e. the computer bureau.

There are many similarities between the principles underpinning the computer bureau of the 1960s, and today's Cloud computing services. A key difference however is that the largest Cloud computing providers operate on a much larger scale, provide a much broader range of capabilities, and have potential to address a greater range of business problems, while considerably lowering costs.

It is generally recognised that Cloud computing services have six common attributes [61]:

- Service based consumer concerns are abstracted from provider concerns
- On demand self-service, allowing service users to unilaterally provision computing facilities without requiring human interaction with each service provider.
- Scalable and elastic, providing access to resources that are "pooled" usually across multiple locations.
- Shared
- Metered by use
- Uses Internet technologies/Ubiquitous network access

4.2 So is Cloud computing just the return of the computer bureau using Internet technologies? If not what has changed?

Over the last 30 years much of the pace in ICT developments has been driven through intersections of technology, media and social factors. This is very true of Cloud computing, which while having significant parallels with the computer bureau, represents a very different ICT proposition.

Perhaps the most significant change driver is the market orientation. The computer bureau was firmly part of the "business services sector", and focused on relatively small numbers of high-value business clients who were dealt with through a personal, face-to-face sales and support channel.

Today's leading Cloud computing providers have much more of a consumer markets orientation. Google and Amazon in particular originated with "commoditization" orientated business models designed to service hundreds of millions of consumers. Amazon sells products and services that are sold in volume on an "as is" basis through a low-cost channel. Support services are automated wherever possible.

The "commoditization" orientation underpins the design of the ICT services provided by the large Cloud computing providers. Thanks in part to the consumer orientation, the services and features that "front-line operational staff" need have been prioritized by some cloud providers over and above those required by the CIO or ICT manager [64] [65]. This is bringing benefits such as rapid innovation in areas such as mobile, GPS/mapping, payments etc, and led to initial take up especially by smaller organisations. More recently some cloud providers have added the additional features requested by larger business customers, such as data import/export, devolved administration, audit, security and other features.

4.3 How can using Cloud computing services help businesses?

The need to save time and money are frequently cited as the justification for making the transition to using Cloud computing services. Cloud computing services do not require users to make significant upfront capital investment; the investment has already been made by the service provider. Because cloud services are immediately available, where they can be configured to meet a business need the solution can be deployed far faster than using a

conventional approach (where it may take up to 3 – 6 months just to procure and deploy new hardware in the data centre).

Longer term, organisations report other benefits too. For example, the collaboration capabilities in Google apps (eg "Google Hangout" group video conferencing and shared editing of a document) enable new, less costly and more productive ways of holding meetings. The mobile device support available as standard with some cloud services eliminates what had previously been a complex and costly process of configuring services to be accessible from multiple types of devices.

Perhaps most importantly at a time of economic challenge, use of cloud services can enable accelerated innovation. No longer need it take 12 to 18 months to deploy the IT to enable a new idea to be tried out; this can now be done in days or weeks. The investment hurdle can be much reduced; it's more practical to try out new ideas if the ICT enablement will cost you a few hundred pounds per time compared to many tens of thousands.

4.4 What types of service are available?

Cloud computing services are generally considered to fall into one of three categories [61]:

A. Infrastructure as a service (IaaS). IaaS services provide access to data centre based resources. These include "virtual machines", typically with access to network resources, storage services, and other capabilities that may include database and system management tools. With IaaS organisations still need to design and configure ICT systems, and do the operating system and application level management. Examples of leading IaaS providers include Amazon Web Services [51] and Rackspace [37].

B. Platform as a service (PaaS). PaaS services provide virtualised hardware provisioned with operating system and related software. They can include a "development toolkit" that makes it easier to design and run a business application than starting from the use of conventional developer tools. Examples of PaaS include Google app engine [15], which Google describe as "making it easy to write an

application that runs reliably, even when under heavy load and accessing large volumes of data".

C. Software as a service (SaaS). SaaS provides "ready to use" business services for specific tasks. Some SaaS services provide standard services for example e-mail and access to word processing and spreadsheet facilities. Others can be used as platforms for more complex "line of business" type applications;- for example salesforce.com [16] provides a customer relationship management application that can be configured for individual organisations.

4.5 Cloud deployment models

The US National Institute for science and technology (NIST) has identified five possible Cloud computing deployment models, with the expectation that users will progress to the "higher" levels as the maturity of cloud providers and consumers increases:

- Level I: Private cloud, where the cloud infrastructure is owned or leased by a single organisation and is operated solely for that organisation. An example is Bechtel [43].

- Level II: Community cloud, where the cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns, e.g. UK government's citizen facing services. SITA provides an example of a community cloud service [53].

- Level III: Public cloud, where the cloud infrastructure is owned by an organisation selling cloud services to the general public, or to a large industry group. A leading example is Amazon Web Services [51].

- Level IV: Managed cloud, where the cloud infrastructure is provided by a designated service provider and may offer either a single tenant (dedicated) or multitenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure can be owned and physically located in the consumers or the service provider's data centres.

- Level V: Hybrid cloud, where the cloud infrastructure is a composition of two or more clouds that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

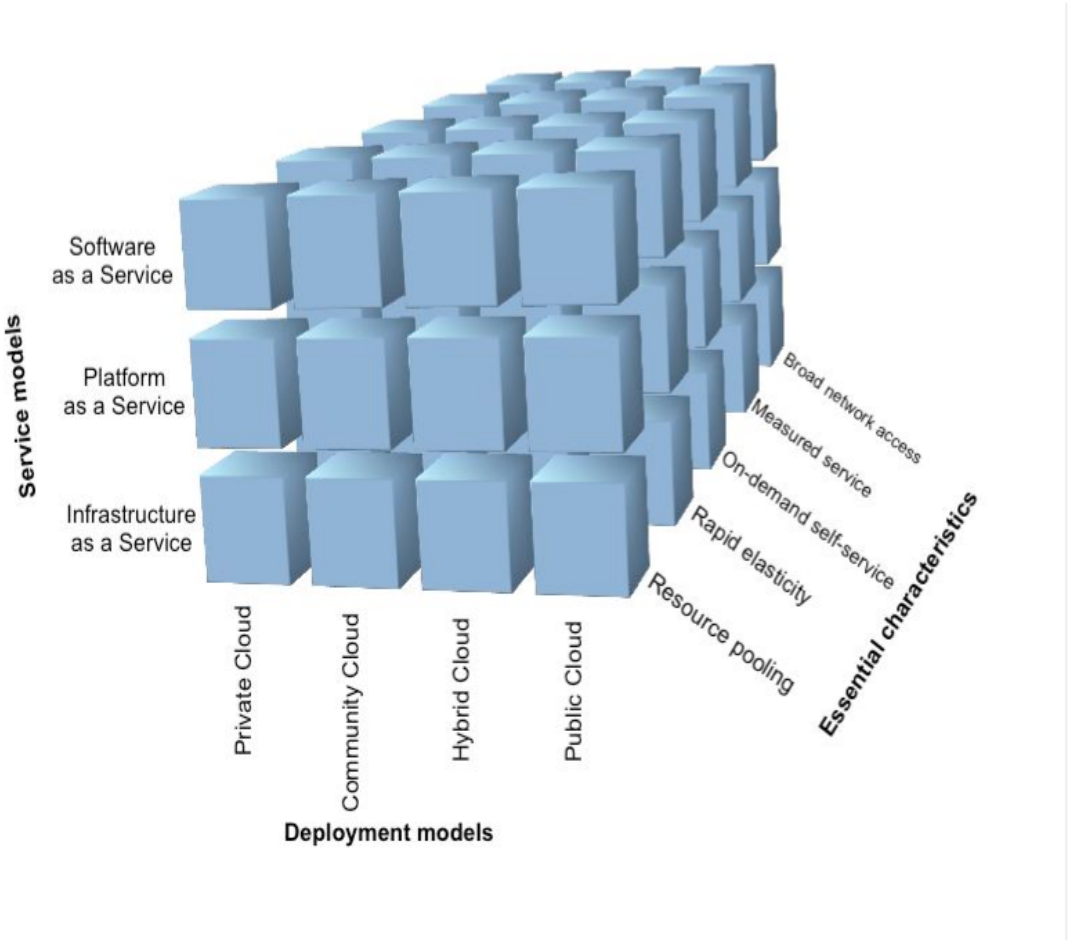


Figure 1: NIST Cloud computing definition (diagrammatic representation)

While some Cloud computing services have developed using infrastructure initially designed for consumer focused commercial services, an ever-wider range of services is becoming available and they are increasingly used by businesses.

Although many organisations are now making significant use of Cloud computing services, in larger organisations current usage (2013) tends to augment rather than replace conventional ICT services. There are however an increasing number of examples of successful 'mainstream' scale Cloud computing deployments (more than 50,000 users) in large organisations; for

example the Dutch supermarket group Ahold [14] and the Spanish bank BBVA [15] are both using the Google Apps service to deliver collaboration services, e-mail and office applications to employees globally, while Japan Post is using salesforce.com [16] to provide front-office transactional and information services on a national basis.

4.6 ICT as a utility

The catalyst for the creation of some of today's large-scale Cloud computing services was the business models of some of the then emerging large consumer facing Internet firms [66]. In such commercially driven environments, optimising sales revenue is critically dependent on being able to provide applications that will attract large numbers of consumers, from whom revenue can then be generated. However, it can be hard to predict what the "winning applications" will be next quarter, let alone next year. Meanwhile the prizes go to those organisations that can address the needs of tens of millions of consumers. Providing new ICT infrastructure at this scale can involve lead times of many months; extending to more than a year if new physical data centre capacity needs to be constructed. This presented the consumer Internet firms with a dilemma; how to quickly provide large-scale infrastructure for applications that have not yet even been conceived? Their solution was to separate the detail of "consumer concerns" from those of "provider concerns", through using software virtualisation as an abstraction layer. Such abstraction is a key feature of today's Cloud computing services;- hardware is organised as a pool of standardised shared virtualised resources that can be quickly reallocated between applications as needed, thus enabling "on demand" scalability.

From the application perspective use of software virtualisation enables new hardware that is purchased to extend data centre capacity to appear (logically) identical to the corporate standard, whereas previously when adding new hardware it would have been necessary to consider whether applications needed to be remediated to reflect specific infrastructure features such as software and even firmware versions. Because all hardware now "looks the same", any physical system can quickly be reallocated to the applications that are generating revenue. The high level of logical standardisation implicit in the approach created an environment where it became affordable to pursue much greater levels of automation of data centre management processes, which also helps drive out human error and thus improve service quality. It was then a relatively simple step to link e-commerce front ends with the systems that support data centre automation to create Cloud computing services that can be sold over the Internet. Effectively,

the computing resources provided by hardware could then be presented as a service, a service that can be sold, provisioned and consumed by applications on demand.

The majority of the largest scale providers of Cloud computing services have thus emerged from the (commercially funded) consumer-focused sector. From the perspective of businesses that use ICT, this simultaneously brings other advantages; analysts have long talked about the "consumerisation of ICT", and such services have taken the lead in "design for usability", for example providing intuitive user interfaces and ubiquitous access on mobile devices. Since around year 2000 it has been ever more common for employees to make unfavourable comparisons [67] between what can be seen as expensive and outdated ICT in the workplace, and the 'free to use' services available to everyone as consumers, for example on a smart phone that can be bought for a few hundred pounds. The affordability, utility and quality of such services has led to mass market take-up, with by December 2013 there being an estimated 1.2bn smart phones in use globally [68]. Some of the large Cloud computing providers are generating substantial advertising and commercial revenue from this large and growing user population, thus justifying further investment in service development, and creating a virtuous cycle.

Other enablers in the development of Cloud computing services include the widespread availability of broadband networks, and standards that enable service interoperability on devices. Analogies have been drawn between these enabling factors and those that underpinned major economic shifts such as the industrial revolution or the development of the electricity grid.

4.7 Getting data in and out of cloud services

The majority of cloud services enable organisations to store data. For example Amazon Web Services provides a variety of database and storage capabilities, and offers a range of data transfer capabilities including accepting physical media for download.

When using such approaches it is important to understand what happens at the end of the contract with the cloud services provider, i.e. how to get the data back again? Leading cloud providers recognise that making it possible to "switch easily" is a key element of marketing strategy, and a variety of techniques are available. Google apps for example will assist with transfers of e-mail content back to an on premise service; Amazon offer a variety of options that can include transfer on physical media for large volumes of data.

Organisations may choose to hold data internally for a variety of reasons, for example so that a single customer database can be used to underpin a variety of on premise and cloud-based applications, or to provide greater control over data as the gateway can restrict the number of records accessed per hour (thus reducing risks such as theft of a large file). Many Cloud computing providers offer a secure interface for access to such data via the corporate firewall. Such providers include salesforce.com that provides a high volume transaction interface that us used by Japan Post [16] that uses salesforce to provide 'front office' services for its many millions of user accounts, while retaining account data on an internal database with this being called as required via the gateway for front office use.

4.8 Challenges in using Cloud computing services

Cloud computing services can be complex to use, and trust is required in the providers. The combination of these factors, coupled with lack of detailed control over how the cloud provider designs and manages its systems means that many potential users perceive that there are significant risks in using Cloud computing services. Frequently cited risks (reference Gartner) include:

- Inability to assess the risks inherent in the cloud vendor
- Unknown data location
- Lack of portability of data
- Lack of portability of code written for a particular cloud provider
- Loss of data
- Breach of data security
- Vendor ceases to be commercially viable.

Managing these risks effectively, while still preserving the benefits of the Cloud computing approach represents a challenge. For example if a cloud provider ceases to meet expectations how practical is it to get an organisation's data back from the cloud provider, in a format that can be reused internally or by another service provider?

4.9 Chapter conclusion -- Cloud computing is by no means a new concept

The concept of utility computing is over 50 years old, and is relatively well established for some

community services, for example air ticket booking, ATM sharing etc

The “client/server” era of the 1980s to 2000s led to a proliferation of servers and data centres, moving the industry away from the benefits of utility computing. Addressing each new business problem tended to result in a new ICT solution, requiring new servers with a unique software configuration, leading to proliferation of large numbers of systems with low utilization levels. Over time the inefficiency of the approach became progressively more apparent. Starting from the late 1990s, organisations such as salesforce.com began to show that “multitenanted” services could again yield higher levels of efficiency and lower unit costs, as was the case for the computer bureau in the 1960s.

5.0 The benefits proposition

5.1 Introduction

Previous chapters set out how, from the perspective of businesses, Cloud computing services have the potential to enable:

- Reduced ICT costs.
- Better ways to innovate to improve customer value propositions.
- Creation of new ways of doing business, leveraging Cloud computing.
- The ability to deliver to mobile devices with rich user interfaces, with a range of tools such as integrated mapping enabling rapid "catch up" with users' expectations of what modern workplace ICT should be providing.

Previous sections have also described that, particularly for more complex applications, the costs of using Cloud computing services can be substantial. If a user organisation has to scan the market to assess many thousands of competing providers, and then do a detailed assessment of shortlisted services on criteria such as functional fit, non-functional requirements, data standards, disaster recovery, peak load performance, data location etc the costs will be substantial. Furthermore, potentially much of this work will have to be (perhaps almost continually) reassessed; as Cloud computing providers routinely update their services. The challenge becomes even more complex where a business need is addressed using two or more Cloud computing services, where the interactions also need to be taken into account. Finally, exit costs also need to be considered, including the practicality of being able to obtain access to organisational data and transition this to a new provider in the event of dissatisfaction with the chosen Cloud computing provider.

5.2 Potential benefits

While the potential for cost reduction is often the first benefit cited for Cloud computing services, we found that careful analysis is needed in each case. Although the "list price" of Cloud computing services may appear low compared to current ICT costs, it is essential to ensure a like-for-like comparison is done. For example are configuration and support costs included?

We identified that together, the combination of tools that enable organisations to work more effectively, and those that can accelerate delivery of market leading customer propositions can boost the pace of innovation. There is potential therefore for early adopters to enhance their competitive positioning and thus future growth prospects.

The core purpose of ICT is of course to enable the effective use of information, and there are many examples (such as social networking) where information is shared across users, and thus where the value of a service is enhanced as the number of users increases. Cloud computing services are advantageously placed to underpin services where such “network effects” apply, i.e. where information is shared across a business community. In the UK public sector there is increasing focus on encouraging local collaboration between public sector organisations to achieve better focus on particular citizen groups or business segments. A shared secure cloud-based service has the potential to provide the ICT needed for such initiatives on an “on demand” basis, with rapid decommissioning when the goal has been reached.

Some product-based organisations, for example aircraft manufacturers, have been shifting their customer proposition from “product” to “service” over the last decade or so. For example data on modern jet aircraft engines is routinely collected by the manufacturer after every flight, with maintenance and servicing automatically scheduled by the supplier to maximise safety and operational performance. Use of Cloud computing services, together with mobile data networks and interconnected sensors opens up the possibility of accelerating a similar service transition in consumer products, for example automotive, home management systems etc.

The transition to Cloud computing services has the potential to enable a more dynamic ICT services marketplace. The barriers to entry for new ICT providers are lower with the Cloud computing business model compared to conventional approaches. Providers need less investment capital as many of the necessary ‘provider capabilities’ can be purchased as services. Likewise the ability to sell over the Internet, with automatic provisioning reduces costs of sale.

From the perspective of those responsible for procuring business ICT, theoretically the shift to Cloud computing allows easier price comparison, providing services are genuinely comparable. In many cases however we found that comparability is constrained by the lack of a comprehensive set of standards, different measurement methods and the rapid evolution of

services. Similar conclusions were reached by Miranda Zhang et al in their paper Investigating Decision Support Techniques for Automating cloud Service Selection [18].

5.3 Financial benefits

Looked at through the ICT lens alone, it can be argued that for large organisations the financial benefits of Cloud computing may be marginal after they have been offset against the additional costs incurred in managing the inherent risks.

Possible advantages of reduced expenditure on applications, infrastructure, power and staffing have to be weighed against security concerns, dependence on Internet connectivity, and the difficulty of customising applications to meet precise business needs. Indeed even the cost advantage becomes debatable if the comparison is made with leasing; is Cloud computing exchanging reduced upfront costs for higher service charges across the lifetime of the contract-making for increased expenditure overall?

Other assessments confirm that smaller organisations tend to enjoy greater percentage savings from using Cloud computing services; for example a study by Hurwitz and Associates [38] found that
‘’Overall TCO for NetSuite’s cloud-based integrated solution suite is significantly lower than a comparable on-premise solution consisting of Microsoft Dynamics GP and CRM. This holds true for both SMB and mid-market firms. The TCO for cloud-based vs. on-premise business application solutions was: — 55% lower for 52 users — 50% lower for 100 users — 35% lower for 200 users.’’

However, while the above "marginal cost" argument may apply to some hyper efficient organisations, for many, today's "unique hardware for every application" reality has catalysed gross inefficiency in the datacentre. It is not uncommon to find huge over provisioning of infrastructure for key applications; this has not happened as result of a deliberate desire to waste money, but rather from a project centric determination to do the right thing for the business, and to invest in:

- sufficient core production infrastructure to ensure adequate application performance during the busiest hour of the busiest day of the year.
- disaster recovery infrastructure that duplicates the core production infrastructure in case the first ceases to be available.

- a volume testing platform that enables representative load tests to be done on new releases prior to deployment.
- various additional development and testing platforms.

The net result of the above can be that up to five times the infrastructure capacity needed to support the “peak hour” load is put in place for each application.

With a Cloud computing based approach, theoretically it becomes possible to achieve substantial savings in resource allocation firstly by:

- provisioning only the capacity needed for the production infrastructure, and then by dynamically flexing this up and down during the working day, week, month and year.
- Sourcing the infrastructure needed for disaster recovery, development, volume test etc on an on demand basis, and releasing this capacity when not needed, including overnight for development systems.

Thus the investment made by cloud providers in a standard virtualisation model (that enables any workload to run on any machine), and the automated tools to enable allocation and release of infrastructure capacity to workloads within a few seconds, enables cloud to achieve much higher utilisation of data centre equipment then is feasible in a conventional enterprise environment.

This model is embraced for example by Amazon Web services, with a pricing model [69] that allows capacity to be requested “on demand” with a (near) guarantee that it will be provided when needed, a discount for “reserved instances” where there is commitment to use capacity on a long-term basis, and a “spot price” for capacity needed for non-time critical tasks. The latter pricing model enables users to specify the maximum price they are prepared to pay; capacity will then be allocated firstly when available, and secondly when not pre-empted by a higher bidder.

Of course large organisations could invest in comparable degrees of automation, and across a large enterprise could aspire to achieve similar levels of system utilization. But this would come at the cost of significant investment in technical and organisational capability, requiring dedicated management focus. As is the case with most activities, it can be argued that it is best to outsource such activities to “the experts”, and focus on leveraging an organisation’s “core competencies”.

There are a number of published case studies on the cost reductions achievable by moving from "on premise" to "software as a service based solutions". For example in IEEE software, [39], Katsaros and Bozanis have published a study that argues that a transition to SaaS client services can reduce customisation, capital and operational costs.

In this paper, the authors report on a study of the total cost of ownership of a combined ERP and CRM package for around 600 users (200 concurrent). The study compares ownership costs over a period of one year, five years and ten years, looking at a conventional on premise solution compared to both a software as a service and infrastructure as a service cloud offerings. What is evident from this study is that significant savings are achievable through the move to use of cloud services. Compared to on a premise solution, the software as a service option provided savings of approximately 66%, 50% and 40% over the one, five and ten year comparison periods. By comparison the savings for the infrastructure as a service option were approximately 50%, 55% and 60% over the same periods.

Interestingly, the relative merits of SaaS and IaaS vary depending on the time horizon; while the SaaS option offered the greatest savings over the short term but then saw the savings decline in relative terms, the IaaS option provided the larger savings over the longer term, with the proportionate savings continuing to increase over time.

5.4 The business reinvention possibility

Creative exploitation of Cloud computing services enables new ways of doing business. In an article in the European Business Review titled "understanding the business impact of Cloud computing", Wilcox, Venters, Whiteey and Hindle [40] argue that use of Cloud computing services will result in

- Greater emphasis on service performance
- A move from products to business services (and)
- Transformative reconfiguration of the supply industry

The authors argue that there will be growing expectation that metrics will be published enabling customers to assess the performance of cloud providers.

More significantly, they make the case that the availability of "on demand" computing power will raise consumer service standards, and thus expectations, citing for example the provision of services to Qantas's 7 million frequent flyer members.

For the longer term, they expect changes in the structure of the ICT industry, with a shift towards:

- A relatively small group of bulk providers of utility and platform services such as storage, processing and e-mail.
- A much larger group of specialist providers with distinctive industry or functional expertise, that will increasingly provide entire "business processes as a service".
- A more elite group of service integrators with deep consulting and technology skills who will partner with enterprises to design, manage and optimize the services ecosystem.

The arguments made in the article "understanding the business impacts of Cloud computing" are highly aligned with earlier work published in 2000 by Ravi Kalakota and Marcia Robinson in eBusiness 2.0 [41].

Kalakota and Robinson set out the case that the internet makes it possible for "business webs" of suppliers, distributors, service and infrastructure providers to collaborate in providing services to customers using the Internet as the basis for business communication and transactions. They argue that "business model innovation", that exploits the "power of business webs" will progressively, industry by industry, destroy the old model of the firm. They cite the work of Nobel Laureate economist Ronald Coase who some seven decades ago posed the question "why do firms exist?", and who identified that transaction costs are the basis of the contradiction between the theoretical agility of the market and the durability of the firm. Transaction costs have three main elements:

- Search costs, the cost (time, resources, out-of-pocket costs, checks) involved in finding a supplier
- Contracting costs, the overhead involving negotiating price and setting a contract, which for small transactions can exceed the value of the deal
- Coordination costs, the cost of coordinating resources and processes

Kalakota and Robinson Set out a vision of an integrated e-business architecture that would combine:

- Supply chain management (ERP)

- Selling chain management (CRM)
- Business intelligence
- Employee relationship management
- Stakeholder engagement (via Finance/accounting/auditing)
- Business intelligence

Using “enterprise application integration” tools to integrate the above applications, and “Web services” techniques to dynamically validate and contract with new suppliers (and possibly new employees) creates the potential for firms internally to specialize more narrowly “i.e. excellence in a niche”, and to source the best value support services needed, and change these where necessary, and thus succeed in the marketplace by offering superior “value propositions at lower prices” than established firms.

Since Kalakota and Robinson published ebusiness 2.0 there has been substantive change in some industry sectors, for example travel, specialist retailing, and with innovation having enabled newer entrants such as Amazon, Expedia, iTunes and NetFlix to gain substantial market share. Other industries, for example petrol retailing, and food distribution have changed at a slower rate however. In general, we have not yet seen the emergence of the dynamic economy foreseen in eBusiness 2.0, due to factors such as:

- The continued importance (indeed arguably growing importance) of brands in signifying trust. Specifically, brands such as Amazon, Google and Facebook have achieved a level of worldwide recognition and success in approximately a decade; in previous eras such penetration of the consumer markets would have taken many decades to achieve.
- The cost advantages associated with scale have tended to embed the position of the successful first movers, some of whom have then leveraged their scale advantages to provide business services to others (e.g. Amazon providing electronic store capabilities and cloud infrastructure services via AWS, Google and salesforce.com providing application development environments).
- The Internet has substantially enhanced consumers’ ability to discover the best prices available not only nationally, but also on a worldwide basis, which in turn has reinforced the importance of scale economies.

Looking to the future, there are undoubtedly further opportunities to leverage Cloud computing as an enabler of new ways of doing business. For example provision of the more commoditised end of professional services such as accounts preparation and tax assessments.

5.5 Risks and benefits

5.5.1 Risks

Studies have argued that while the inherent risks are not new, the Cloud computing model does potentially intensify their impact [21].

The ‘e commerce’ based Cloud computing sales model creates challenges in assessing and managing risks, Specifically it is generally inappropriate for large organisations to commit to a standard “click to accept” contract; such contracts usually allow the supplier to restrict liability or to change terms unilaterally and this can have unacceptable impacts [37]. Meanwhile the costs of putting in place a bespoke contract with the cloud supplier may be significant, if indeed this possible. Another challenge is managing the risks of information assurance; can the Cloud computing provider’s service be trusted to securely hold the consuming organisation’s data on a “sold as seen” basis, or is due diligence necessary? Even if the provider is well intended, can there be confidence that personnel, procedures and technical protection will be adequate to maintain protection? Challenges are heightened by an asymmetry in the relationship between cloud provider and cloud consumer; the service definition and performance criteria that cloud providers reveal and commit to in SLAs frequently covers only a small proportion of overall service dimensions.

Although use of Cloud computing services can help mitigate some risks, such as obsolescence and capacity management, organisations need to invest resources in understanding and mitigating the new risks that arise. Theoretically, if large organisations are able to adopt just one or two Cloud computing providers for each of their core ongoing business service needs, more effort can be invested in assuring these. However, there are barriers including:

- the cost of assurance,
- the unwillingness of some cloud providers to disclose detailed information, and
- limited supply of the necessary expertise.

Consequently these types of issues are generally resulting in larger organisations restricting the use of Cloud computing services to information that requires relatively low levels of protection, for example internal email and collaboration services, and public websites. [22]

We considered that the main categories of risk inherent in using Cloud computing services [19] are:

A. Information assurance including legal compliance, lock in and aggregation risks

When using a third-party ICT provider, confidence that an organisation's data will be available when needed and not inappropriately disclosed to a third party depends on a combination of robust technical, procedural and personnel controls. Whether these have all been developed and applied effectively cannot be verified without extensive dialogue with the vendor, and with a Cloud computing service this is often impractical. Establishing trust in a context where there is not a personal relationship between vendor and customer, and where there is no regulation or agreed industry standards, presents a real challenge.

Cloud computing services are often provided on a global basis, and data, or user identity verification information may flow outside national borders. It's important to understand any legislative requirements such as the need to keep data within a particular geography, and to ensure the cloud provider is able to fulfill these.

With conventional "on premise" delivery models, it is by no means unusual to find that dependencies on particular vendors have grown to the point where there is no realistic alternative but to continue to invest in non-discretionary upgrades. The same risk exists with Cloud computing services; innovating by exploiting vendor unique features to improve services simultaneously creates the possibility of "lock in" [70], which in turn leads to the risk of exploitative behavior on behalf of Cloud computing service providers.

Corporate ICT functions generally manage risk by identifying business critical services, and ensuring that these are not vulnerable to "single points of failure". This is practical (albeit difficult) where the service topology is fully under the control of the consuming organisation. While the use of Cloud computing services may appear to diversify supply and thus reduce such risks, there may be unforeseen points of aggregation; for example if a "backup service" is selected, is there confidence this is not in fact hosted at the same physical data centre as the live service?

B. Service functionality and standards.

Cloud providers innovate through the addition of new features; generally these are prioritised by the provider to optimise market share and future profit. From the perspective of a specific user organisation, this creates the possibility that services selected because of current fit with business needs cannot be guaranteed to do so in the future.

C. Service management risks.

Some cloud providers provide service guarantees that are based on assumptions on the peak simultaneous usage level generated by customers. Should anticipated usage levels be exceeded then service degradation occurs, with many providers then offering a rebate of charges. While financial compensation alone may be acceptable for some services, this is not the case for services that are genuinely business critical. Hence the attributes to consider include the service design capacity, as well as factors such as failure recovery time, whether a disaster recovery facility exists and fault resolution SLAs. The ethical integrity of the Cloud computing service providers' management team is also important. Most will seek to provide the capacity that is needed; some may decide that it is more financially profitable to tolerate regular degradation, and to pay financial rebates to those customers who observe the degradation and put in a claim.

NIST has observed that new service risks that arise from the unprecedented complexity and scale of some Cloud computing services. Such factors create "new risks of service failures resulting from sequences of events that are difficult to predict, where the consequences can be significant, and for which substantial time may be needed to diagnose and repair outages". An example of such a failure is the outage that impacted Amazon EC2 in April 2011[24].

5.6 Chapter conclusion -- Cloud computing has potential to bring substantial benefits to large-scale enterprises through economies of scale/lower unit costs.

As a consequence of the risks set out in this chapter, the starting point for using Cloud computing services in most organisations will generally be for relatively simple services; these may include the use of in-house "private clouds", supplemented by the use of public cloud services for non business critical activities where risks can be managed; for example

development and test services, or collaboration with other organisations. These “use cases” however only account for a relatively small proportion of ICT spend.

Potentially much larger benefits can be obtained if cloud services can be applied to automate core high-volume business processes, as, in most large organisations, these account for the majority of ICT costs. Doing so however will typically require the use of a mix of in-house services (e.g. authentication services, access to data), and the use of a range of external services integrated with case management, with business rules applied to determine the next step in the transaction.

The distinguishing characteristic of transactions is that if they do not complete in full then all the steps need to be “unwound”, and the orchestration process that combines the use of in-house and cloud services will need to accommodate this essential requirement.

“Soft issues” represent a major barrier, for example most organisations lack the capability and in-depth knowledge base needed to be confident that the risks of using cloud services for core business processes can be effectively managed. For example there are significant concerns over compliance issues, including preserving information security, and avoiding unintentional breaches of legislation.

Part 2: Identification and analysis of foundation capabilities needed for widespread utilisation of Cloud computing services

This section is based on the high-level design work that was undertaken on the UK government cloud proposition (from mid-2009 to mid-2010).

As set out in chapter 3, during the period September 2009 to April 2010 I initiated six "definitional" work strands that defined the target future state for government use of cloud services (vision), the high-level technical architecture, the approach for holistic management of a portfolio of cloud services, the strategy for maintaining security of information, the commercial strategy and the high-level business case.

As Programme Director, my personal contribution to this phase of work was to:

- Design the eight workstrand structure of the research programme,
- Identify that a volunteer based approach could be a viable mechanism of sourcing the resources needed to undertake such a research programme,
- Invite volunteers from both government departments and the ICT industry to join the research programme, on the basis that volunteers would be expected to work free of charge on a four day per week basis for a four-month period,
- Promote the programme to encourage volunteers, presenting to government departments and ICT firms, attending meetings and presenting at industry gatherings,
- Once initial government volunteers had been identified and selected, to form a programme team, to appoint leads for each workstrand, and to draft and then agree the terms of reference for each workstrand with the workstrand lead,
- To orchestrate the process through which suitably skilled volunteers were allocated to each workstrand, including the appointment of an "industry co-lead" to each workstrand,
- Chair a weekly "programme team" meeting that managed overall progress, that identified and resolved interdependencies between the workstrands, and which (in rotation) reviewed in detail the emerging themes from each workstrand's deliberations (NB: For example the interfaces depicted in Figure 3 were identified during a joint programme team review of what is needed to automate the deployment of cloud computing services

selected from an on-line catalogue, in the context of the user organisation's business, data, network and desktop contexts),

- Meet with each workstrand lead on an individual basis approximately every four weeks to review progress,
- Conduct a in-depth review of the Service Management workstrand, resulting for example in figures 5 and 6,
- Review the draft report produced by each work strand, personally signing each off as programme director,
- Prepare and acting as the executive for the monthly programme board that was chaired by the CIO of the Ministry of Justice, and attended by the Government CIO,
- Personally present progress reports and ultimately recommendations at three meetings of the Government CIO Council in the period Autumn 2009 to spring 2010.

Additionally I co-authored the Service Definition workstrand report [19] (which defined the business vision).

The following chapters set out the conclusions from this phase of work, covering:

- the business vision.
- the benefits of transitioning to the Cloud computing model.
- the constraints that need to be overcome to realise the business vision, and the costs involved in doing so.
- the implications of the transition for people working on ICT;- eg within government departments, within ICT suppliers.
- from who is support is needed to make the transition, and the benefits case for the various stakeholder groups.
- how to catalyse getting the transition underway so that it will be sustainable and will progressively build pace.
- further elaboration of the risks that need to be managed.

6.0 Future ICT operating model based on utilization of cloud-based services

This chapter summarises the work of the G Cloud Service Specification team between October 2009 and April 2010 [19]. The team consisted of representatives from government departments and the ICT industry;- the team provided regular updates of its work to the G Cloud programme team which reviewed, moderated and directed its work.

6.1 Context for public sector ICT

ICT as an industry has evolved rapidly over the last 30 or more years, with the development of personal and client/server computing, the Internet, mobile technologies and enterprise applications covering supply chain management, financial management and customer management being just some of the areas that have progressed.

The “first mover” benefits available to organisations that achieved early successful deployments of new technologies have often been substantial, and this has contributed to an environment where a race to leapfrog the competition has become the norm, resulting in diversification of technologies.

Citizens’ perspectives of rapidly developing and improving services from private sector organisations in the 1990s and beyond led to pressure for public services to be improved. By the early 2000s this had resulted in an increased pace of change for public sector organisations, but with the consequence of accelerating diversification of ICT systems.

With the economic crisis beginning in 2008, priorities in the public sector changed, and there has since been increased emphasis on cost reduction. When the consequence of past generations of public service improvement projects was assessed in the round, it became clear that the parallel focus on multiple projects that had been progressed in isolation had led to huge duplication at many levels. This applies to infrastructure, applications, data standards, service designs, citizen experiences etc. Across the public sector hundreds of networks and data centres, and tens of thousands of severs and business applications have been put in place, with many overlaps. From this perspective alone it is clear that considerable rationalisation and cost reduction is possible.

However, ICT rationalisation is easier said than done. The rapid development of the ICT industry's products and services, together with an increasingly distributed approach to developing business solutions has, at the detailed level, led to different approaches to solving the same problem; for example different network protocols, different data standards etc.

Nevertheless, the rapid development of the Internet has accelerated adoption of networking standards (IP) and browser display standards (HTML). This has removed a significant barrier to enabling the reuse and integration of services that increasingly can today be readily displayed on the same device and share the same network. This contrasts with the position prevalent in the 1980s, when many suppliers had their own incompatible networking standards such as IBM's SNA, while before the prevalence of HTML/Internet browsers vendors of information services often needed to deploy of their own unique "terminal" (or "PC display software").

By 2008, government had already declared its intent to consolidate and standardize ICT networks, and to establish a strategic "end user computing" strategy that would establish common standards for the devices used by end-users. These initiatives create a context that eases the transition to a Cloud computing based model for sourcing information services.

6.2 It is Cloud computing a fad or an "industry inflection point"?

These issues were considered by the G Cloud programme's service specification team when we set out a proposed "future end state" for use of Cloud computing amongst public sector organisations.

Our conclusions were:

- There is evidence that some large organisations have realised significant benefits in the areas of cost reduction and business agility through the adoption of Cloud computing models.
- The ICT industry is migrating towards Cloud computing; following the proven success of the delivery model at high profile firms such as salesforce.com and Google. It has become clear that established "enterprise class ICT vendors" such as HP, IBM, Microsoft, Oracle and SAP are re-orientating their product strategies to leverage the cloud model. For example, an article reporting Oracle's adoption of the Cloud computing model is referenced at [58].

Hence our conclusion was that Cloud computing represents "an industry inflection point" that will result in improved services and reduced costs. As the benefits proposition of the Cloud computing model continues to improve compared to conventional "on premise" delivery models it will become a question of "not if, but how and when the public sector adopts Cloud computing."

6.3 What is the likely timescale within which the switch to Cloud computing services will occur?

We took the following factors into consideration:

- Cloud computing is based on relatively mature technologies; the innovation is based on adoption of commercial models and approaches that enable these to be deployed at scale and shared systematically, rather than the technologies themselves.
- There are however constraints; public cloud services are relatively new and are evolving rapidly. The prime focus of many of the providers is on providing an "free to end-user" (advertising funded) service where agility and rapid information service innovation are critical to competitive success. Providers working within this commercial context may not give the level of priority to aspects that are critical in the corporate and government markets such as information security, and providing high levels of resilience and support to consumers of service.
- Many existing government applications have not adopted Internet standards, and so cannot be readily migrated to public Cloud computing services without extensive "remediation work"; which may be time consuming and costly.
- Successfully using Cloud computing services requires a new approach to the management of ICT. However, the staff working in government ICT organisations, and the corporate ICT profession more generally, are skilled in the "waterfall" approach of "design, build, test, run, support", rather than in the selection and integration of existing cloud services. The leadership challenge of changing the way ICT organisations operate is substantial and should not be underestimated.
- Many government contracts have been let to suppliers for periods of 10 years or more, and migration to adopt cloud services may be more practical at the end of these contracts rather than in "midflight".

Our overall conclusion was that while the migration to Cloud computing services can start almost immediately, a blend of approaches will be needed to accommodate the different characteristics of government ICT services, including both "hard" factors such as the technical standards in use,

and “soft” factors such as each organisation’s information risk appetite and existing contractual commitments. Overall the transition to adopt Cloud computing services should be regarded as a “journey” that will probably take 10 years or more to conclude. Various analysts have independently advocated similar phased approaches [12] [13].

6.4 Defining characteristics of the expected “end state “model for government use of Cloud computing services

Taking the above into account therefore, we proposed that the defining characteristics of the “end state “model for public sector use of Cloud computing services should be as follows:

- Procurement of ICT will switch from a “business solution orientated” model to a “commodity services procurement” approach. In most cases innovation will be achieved primarily by new configurations of existing services, and integrating services in new combinations, limiting work on creating new service(s) to that which is essential to address the unique business challenge in question.
- The commodity ICT services that will be procured and consumed by public sector organisations include “software as a service”, “infrastructure as a service”, and “platform as a service” capabilities that will provide common services such as user and citizen authentication, document scanning, archiving and production, and banking services (usually collect or make payment).
- In the near term these services may need to include some procured specifically for government in order to meet critical business requirements such as avoiding dependence on data centres outside the UK for critical public services, and protecting the confidentiality, integrity and availability of information. Wherever possible though (assuming price competitiveness) the preference should be to select existing public cloud services where these meet business requirements (both functional and non-functional requirements).
- A recognised principle of procurement is “the more you buy, the lower the unit price will be”. A key objective therefore is to enable consolidation of demand, and for this reason we proposed that there should be a published catalogue of services enabling public sector organisations to purchase access to existing services where these meet business needs. This (online) catalogue has now been launched as the UK Government CloudStore.

- In parallel innovation should be encouraged, both through being open to new providers and to new services. This can be best achieved through providing regular opportunities to new providers to promote services to the public sector via the CloudStore catalogue.
- Ensuring services are “easy to buy” will be imperative in accelerating the shift to the cloud model. Any public sector procurement over the EU single tender limit (approximately £110,000) needs to go through a competitive process which involves significant overhead, and which can take many months. The goal therefore should be that services on the CloudStore have already been procured for use across the public sector, and thus that the due diligence on the vendor, the assurance that the service meets defined information accreditation requirements, and the price have all been predetermined.
- Implicit in the approach is that services are offered on a “pay-as-you-go” basis, without consuming organisations needing to fund capital expenditure.
- Incentives should be put in place to maximise reuse of existing public sector ICT assets where appropriate.
- The online catalogue, CloudStore, should provide integrated access to related common public sector services including the Public Services Network and end user computing services, making clear what is, and what is not compatible.
- CloudStore should provide integrated access to both standard public cloud services, and "private" cloud services that have been specifically designed for the public sector.
- Thus, for public sector organisations, CloudStore should offer clear benefits in the areas of faster procurement of the ICT services needed to meet business needs, lower prices, and lower deployment costs resulting for example through the pre-accreditation of compliance with information assurance policy, and predetermined commercial terms.

6.4.1 G Cloud Vision

In summary, the G Cloud vision we set out in 2010 was to establish a public sector “brand” for “ready to buy” information services that will

- Bring “utility convenience to public sector ICT” through provision of shared, flexible and agile, transparent and efficient allocation of ICT when it’s needed, with sharing of standardised resources to reduce costs.
- Deliver the new commercial model that enables public sector organisations to pay for the services they need at the time of consumption.

- Encourage adoption of common standards, removing barriers to sharing information between public sector organisations where there is a business need to do so.
- Provide a range of infrastructure, software and platform services.
- Be pre-accredited to defined standards that make clear the levels of protection to ensure confidentiality, integrity and accessibility to information and ICT-based services.
- Be readily accessible through CloudStore, the shared online catalogue.

It was envisaged (in 2010) that the CloudStore would comprise a mix of private cloud services built to meet government's requirements (and reserved for use by public sector organisations), as well as access to public cloud services. While it was recognised to be preferable to use public cloud services where suitable services are available, the lack of maturity of standards for describing services, and achieving interoperability, security and business service management meant that it was envisaged that services involving sensitive data would likely transition to private cloud services. Nevertheless the ability to share these capabilities across departments, and to share component services (e.g. citizen authentication) still meant that there was scope for considerable cost savings from transitioning services to private cloud.

The proposal assumes automation of some of the enabling services involved in delivering both public and private cloud services; for example once a private cloud service has been selected from the CloudStore, the expectation was that it's instantiation and integration with purchasing organisation's network, data and service management capability would to a significant extent be automated. Such automated tooling was considered essential if the catalogue price of G Cloud services was to be lower than conventional ICT supply routes, although of course this would require significant investment upfront.

6.4.2 CloudStore vision

In the context outlined above, the CloudStore was positioned as:

- Being the marketplace for ICT services for public sector organisations
- Enabling focused and more cost-effective purchasing of certified ICT solutions with emphasis on re-use and on the sharing of applications and services.

6.5 Survey of local authority ICT leaders expectations on cloud services adoption

In April 2010 we conducted a survey of approximately 16 local authority ICT leaders that identified:

- The cloud services identified most likely for “first use” were:
  - e-mail (70%),
  - desktop applications (50%),
  - authentication services for employees and citizens (20%), collaboration tools (20%),
  - computer-based training (20%) and
  - archive services (20%).

- Infrastructure services seen as suitable for use by local authorities include:
  - storage (70%),
  - disaster recovery, (70%),
  - common services (70%) and
  - development/test environments (60%).

- Local authorities considered that some of their existing services could be shared with other organisations using a cloud model, and expected this to be most prevalent for:
  - HR,
  - legal,
  - procurement and
  - payment services.

In summary, this survey identified that the local authority ICT leaders were anticipating that initial use of Cloud computing services would be for relatively uncomplicated and commoditised business requirements; i.e. those where a common Cloud computing based offering can readily meet the needs of multiple organisations "as is". While this represents a pragmatic approach, the implication of the survey is that local authority ICT leadership was not expecting early adoption of Cloud computing services to underpin the more complex organisation specific "line of business" business processes. As discussed elsewhere in this thesis, it is the line of business processes that represent the majority of public sector ICT costs. Hence the significant conclusion from this study is that local authorities were anticipating that the initial use of Cloud

computing services would address only a relatively small part of the ICT expenditure.

As will be discussed in section 14.2, this survey proved accurate in for forecasting the actual "first uses" of cloud computing in the public sector.

6.6 Chapter conclusion -- UK Government is committed to a hybrid cloud 'cloud first' strategy

The published G Cloud vision reasserts the principles of Cloud computing and announces a "public cloud first" policy. It sets out the anticipated benefits of cost reduction and increased flexibility, acknowledges the deployment models of public, private, hybrid and community clouds, sets out the concept of G Cloud being an ongoing programme of work, rather than a single entity, and acknowledges the need for behavioural change and development of the market. This is discussed in detail in Chapter 13.

7.0 Technology – what's needed to deliver the cloud vision?

This chapter draws on both the G Cloud Programme's Technical Architecture Workstrand Report [26] that was issued in May 5, 2010, and on subsequent developments through to September 2012.

This analysis covers

- Context and definitions
- What should a "technical architecture" for deploying cloud services seek to achieve?
- What additional outcomes can potentially be achieved in the future?
- What are the risks from the technical architecture perspective, and how can these be managed?

7.1 Synopsis and summary conclusions

The G Cloud technical architecture considers the relationships and interactions between different Cloud computing services, and the scope for putting in place a systematic framework that could enable automation of service services (particularly within the context of private cloud services).

Using combinations of commodity cloud services to put in place organisation specific processes is relatively complex to undertake, and will be prohibitively expensive if significant human effort involved in considering all the details for each deployment scenario. Automated tooling is therefore needed, both for initial deployment services, and for subsequent ongoing management. We proposed that a standards framework be put in place to enable the following two capabilities:

- **Automation of procurement, acquisition and management services:** so that following the purchase of Cloud computing services offered via the CloudStore portal, services can be automatically instantiated, commissioned (including populated with customers data) and managed. Such automation will require considerable up front investment but potentially reduces the long term costs of acquiring cloud services and switching to new vendors, thus enabling the creation of a more dynamic marketplace.

- **Resource pooling.** The greater the extent to which resources can be pooled and shared across suppliers, and geographic zones, the lower the system resource requirement for providing a given level of service. Theoretically, reducing resource requirements should lower costs. Achieving this however will be subject to containing management overheads, and to the vendors of Cloud computing services not retaining the cost-saving benefits in the form of "excess profit".

7.2 Context and definitions

The objective of a technical architecture framework for the use of Cloud computing services is to provide a common foundation of software and hardware infrastructure principles that can underpin multiple business applications. With the goal of defining a shared platform that can support applications across UK public sector organisations, it considers areas such as performance standards, protocols, services, and the information assurance and other risks that need to be mitigated.

The architecture reflects an objective that was discussed at the G Cloud Programme Board of achieving enhanced value through the integration of both of

- the components (tooling) needed to efficiently manage use of cloud services at scale, and
- the core Cloud computing services in their own right.

This approach was founded on the assumption that while the G Cloud is likely to consist of a combination of public and private cloud services, optimal value would be achieved if purchasing organisations are readily able to benefit from low costs of selection, deployment etc.

7.2.1 Technical architecture definitions

This section uses the definitions covered in Section 4.5, and the following additional terms:

Utility computing is the packaging of computing resources, such as computation and storage, as a metered service similar to a traditional service utility.

Burst computing resources automatically expand and contract in response to changes in application workload.

Elastic resources must be requested by the user, operator or application. Elastic differs from burst in that the application or user must request the additional resources for example via an application programmatic interface (API).

7.2.2 What should a "technical architecture" for deploying cloud services seek to achieve?

The objective set for the workstrand was to define a technical architecture for government cloud and the government application store that reflects:

- Current best practice in the industry.
- Reasonably foreseeable future developments.
- The public sector's "ideal" business requirement.

The original ambition was to achieve "tight coupling" between the CloudStore and the cloud services on offer to enable automated instantiation and commissioning (with the consuming organisation's data) of purchased services.

On reviewing this in July 2013, it is still the case that the standards needed to enable this degree of integration have either not been defined, or become sufficiently widely accepted for this "cloud of clouds" (single logical cloud consisting of multiple vendor services) vision to be a practical possibility. The IEEE is sponsoring work in this area (http://cloudcomputing.ieee.org), acknowledging that today, the standards needed to make federated use of multiple cloud services do not exist.

Current (2013) best practice includes:

- Adopting utility computing models to implement "private clouds", rationalising physical facilities, demonstrating cost reductions and improvements in business agility.
- Selecting public cloud services that can be used on an "as is" basis, for example Google Apps. Progressively driving business value by starting with "business outcome equivalents" of existing services, and then driving additional benefits by making use of the more sophisticated capabilities within the cloud service over time.
- Integrating public cloud systems with back end legacy systems.

Reasonably foreseeable future developments include:

- A diversifying range of public cloud services available at lower cost.
- Greater availability and coverage of "private cloud toolkits", reducing barriers to setting up an in-house facility.

7.2.3 The public sector's "ideal" business requirement.

The vision created by the technical architecture workstrand however goes further, and envisaged standards and tooling that would allow:

- "best fit" infrastructure, application and platform services to be selected (including automatically selected) in near real-time from an online catalogue.
- Automated activation of the services selected via digital interfaces into the operational domain. These interfaces will enable
  - ❖ sourcing of certified software components from a "certified components repository".
  - ❖ automatic deployment of the chosen components on the appropriate infrastructure platform.
  - ❖ automated linking of the customer's data services to the software components, with role-based access and audit controls.
  - ❖ a range of "monitoring services" that will enable service management and billing for services.

To date, there is not an agreed process or timescale on how to achieve this type of automation and integration across public cloud providers, and with private cloud services, so that the service acquisition and management process can be joined up to be "consumer centric" (rather than being "provider centric" as is the case today). Today's reality is that users of cloud services need to handle multiple "supplier centric" services, with SLAs that are provided to different levels of "completeness".

7.3 Standards

Some of the major cloud services and software vendors (eg Amazon Web Services, VMware and others) have developed proprietary standards for their own product sets that enable highly efficient resource pooling and automated provisioning and management within their own domains.

In the context that the total global expenditure on ICT services exceeds £2,000bn pa [71], it is not practical for even a sizeable ICT customer of the size of the UK government (for which the estimated spend is £4bn pa, just 0.2% of global spend), to define standards with which global ICT vendors could be expected to comply. (Arguably it is also not desirable for cloud service consumers to set their own standards, as this is likely to inhibit ability to leverage future industry innovations). Given that there is not the prospect of a pan industry standard for interoperability of Cloud computing services being widely accepted for the foreseeable future, it was concluded that the most practical way forward will be to select the vendors with the most mature capabilities. Additionally there should be support for industry initiatives to achieve interoperability.

Pragmatically, it appears more practical for large user organisations to identify the range of applications and services that are in common usage, and then to consolidate on one or two providers of each, selecting vendors that can demonstrate they offer optimum services and superior “value for money”.

7.4 Technical architecture principles

7.4.1 Service layers

The technical architecture work strand [26] considered the service layers inherent in each type of cloud service. The G Cloud programme board endorsed their conclusions that:

- Infrastructure as a service (IAAS) integrates the following layers: data centre, networking/firewalling, physical servers and the virtualization layer. Only the virtualization layer is presented to the consumer.
- Platform as a service (PAAS) builds on IAAS and adds the operating system layer, and platform/infrastructure software. Only the platform/infrastructure software is exposed to the consumer.
- Software as a service builds on PAAS and adds hosted application software. Only the hosted application software is visible to the consumer.

This is illustrated in the diagram below (figure 2, service layers description) this is reproduced from the technical architecture report [19].

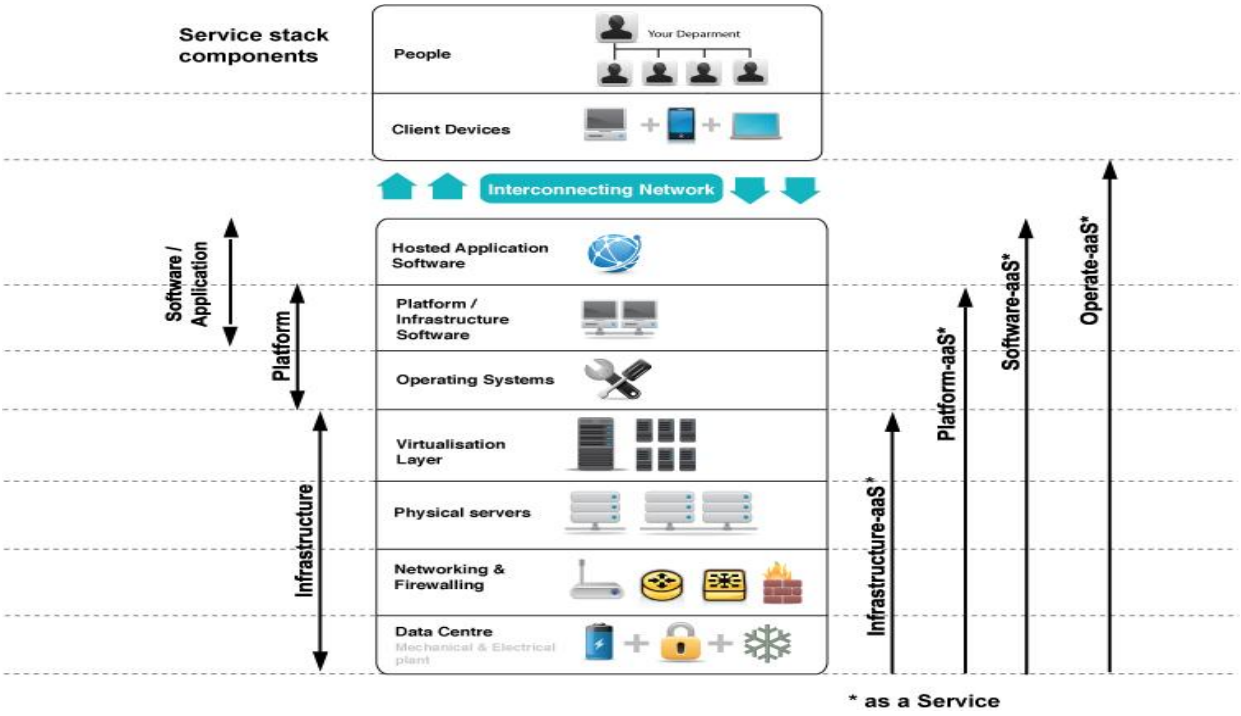


Figure 2: Cloud computing service layers [19]

7.4.2 *Interfaces to enable efficient operation*

To enable systematic use of IaaS, PaaS and SaaS services organisations may choose to define standards and policies for:

- data services, to provide a common secure interface to corporate data
- certified components repository, approved software that can be installed on the IaaS service
- application store, an online catalogue to allow end users to browse and select services
- operate as a service, a set of services to assist with management, building and support of the services portfolio chosen by a user organisation
- interchange and transactions services, to allow interconnections to be made between separate cloud services, and multi-stage transactions to be managed involving successful end to end use of a series of services.

Such automation requires automated transactions (involving sequenced message flows) between different components and services;- this is illustrated in Figure 3 below (reproduced from the technical architecture report [19]):

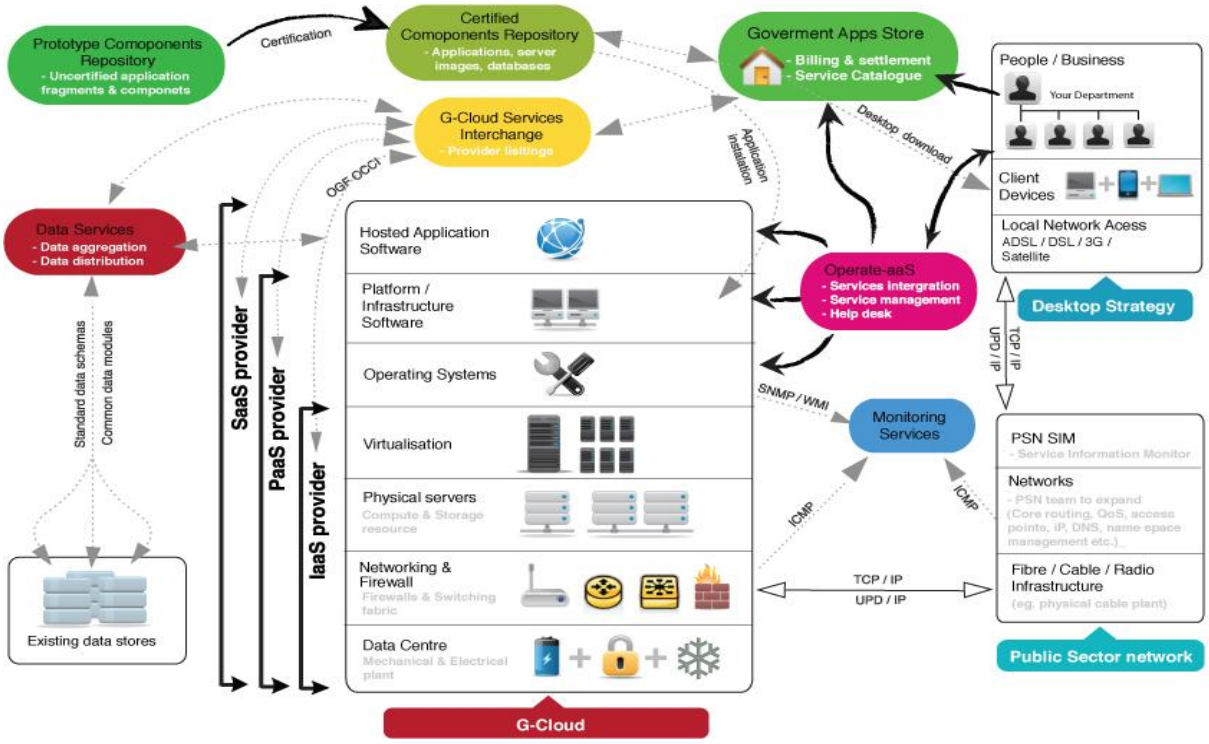


Figure 3: Interfaces requires to automate the selection and deployment of Cloud computing services [19]

Delivering such a capability requires clear and stable definitions for multiple interfaces; covering data standards, core functionality, service management, provisioning etc. The challenges today are that providers offer a different subset of the theoretical range of interfaces, and that interfaces have been implemented to multiple standards.

7.5 Areas for further work by technical architecture work strand

Resource pooling [72] is one of the core potential "value adds "of Cloud computing, enabling resources to be shared across multiple users. The economic model however depends on not all users requiring simultaneous "peak load" access. Inevitably such conditions will arise, albeit (hopefully) rarely. To mitigate the risk of service degradation during such periods the concept of resource pooling with partner cloud providers (or "cloud busting") has been widely discussed, with services such as Eucalyptus [4] providing relevant capabilities.

7.5.1 Desired benefit of resource pooling

It is a recognised principle that pooling of resources between different user communities (and

between different providers) can enable higher levels of overall utilisation, thus enabling further reduction in unit costs.

This has been an element of the "benefits proposition" of Cloud computing since its inception; if resources in a particular time zone are fully utilised excess workload can be relocated to identical underutilized capabilities on a "follow the moon "basis. In principle this avoids having to purchase capacity at each location that would often remain underutilised for the majority of the time.

This involves additional capacity being sought from another Cloud computing provider at peak periods. While some proprietary standards for achieving this exist; for example between VMware users, there is not today a widely adopted open industry-standard for achieving this capability. Such a standard would allow cloud providers to offer "burst" services, creating an additional revenue stream, and helping to mitigate service risk. Such "burst capacity" standards would need to cover areas such as:

- technical capacity (compute, storage, communications).
- request period (large-scale network capacity will be needed to provision such services sufficiently quickly).
- guarantees of non-functional requirements including security, data residency.
- other attributes (eg security levels).

7.5.2 Challenges to be overcome to achieve resource pooling

The services provided by different cloud providers rarely operate to common technical and service standards. For example, what is actually being provided; what type of processor, how much memory? What are the availability targets? Are these measured in a "like a like manner". Potentially, at the infrastructure level, this challenge can be addressed by standardizing resource definitions to a small number of instruction set types, each of which is available with a small set of CPU to RAM ratios. This quickly becomes complicated; this approach can clearly not be extended to proprietary platforms and SaaS offerings. There is also variation in the use of this same terms by different vendors. Achieving resource pooling in a systematic predictive manner will require common terms and adherence to these.

For the longer term the OCCi [59] is intending to define an open API for general use in achieving cloud burstability;- it remains to be seen whether this will be adopted by sufficient vendors to

achieve genuine cross platform integration. It seems unlikely that even if achieved at the IaaS level, that this will be extensible to SaaS or PaaS.

Information assurance is another constraint. For example to meet legislative requirements, or to ensure continuity of essential public services, government organisations may specify a requirement that data remains in the "home country" i.e. in the UK. Potentially this can be overcome by being able to pre-empt capacity needed for "real-time computing services" from the many "batch jobs" that operate, for example for data analysis.

7.6 Potential role for Services Orientated Architecture

In the context that many public services are delivered to all, or a significant proportion of the UK's 60 million citizens, the sheer volumes of data, enquiries and transactions results in the majority of public sector ICT costs being on the provision of services to citizens. This in turn involves many hundreds of relatively complex business services for example "register a birth", "apply for a driving test" and "claim state pension". The current ICT deployment model is to design the ICT enablers for such processes independently, and while all have some unique business logic, the majority comprise common elements such as "authenticate citizen", "capture data", "produce secure document", "collect payment" and "make payment". The G Cloud programme identified the potential for improved outcomes and substantial savings by moving to a model where each of the common services is developed through a managed process, with two or three pan-government sources of supply of each, with such services being described in a catalogue, and available for integration into the business specific processes of each organisation. This ambition is highly aligned with the principles of Service-Orientated Architecture (SoA), with Cloud computing providing an attractive hosting and delivery model that potentially allows SoA-based services to be shared across multiple organisations.

The G Cloud programme recognised that incentives will be needed to maximise reuse of existing assets where appropriate. Such integration brings its own challenges, and we proposed the establishment of a central "authority" (broker) that would set technical and security standards, and ensure that suppliers were validated once for the whole of government. Additionally we proposed that there would be a focus on cloud service brokerage (i.e. selection and deployment) at the "business communities" level (e.g. welfare, justice, health etc), as this creates opportunities for additional value-added services through the provision of community wide services (e.g. data standards, common data repositories etc).

We recognised that the overheads involved in selecting and integrating cloud based “SoA” services would be significant, adding to the costs and timescales of using cloud services.

7.7 Technical architecture risks

A key area of risk from the technical architecture perspective results from established organisations having a substantial investment in a portfolio of applications, typically built over many years, to multiple standards. Taking advantage of cloud services, be they private or public, will present migration challenges. While some services can readily be completely replaced with “ready to use” SaaS equivalents, for organisation specific “line of business applications” there will in general not be 1:1 equivalence immediately available; though with effort it may be possible to recreate services using a combination of PaaS and SaaS.

The most immediately actionable possibilities [73] will often be migrating existing applications to run on IaaS cloud services, although even here there are challenges: to take advantage of the elastic scalability offered by IaaS most applications will require some level of enhancement. At a minimum, business sensitive applications will require retesting, given that performance and availability characteristics can be expected to vary given the different characteristics (published and unpublished) of cloud services.

The above factors will constrain the rate at which existing applications and services portfolios can be migrated to the cloud, although first movers report that it is often possible to migrate comparatively easily 25% to 50% of existing services.

This suggests that careful prioritisation will be essential when planning a cloud migration programme;- the initial focus should be on those applications that can be moved to cloud services relatively easily, and where well defined benefits can be obtained.

7.7.1 Service continuity challenges

NIST in 2011 reported that Cloud computing systems are complex, encompassing (eg [6]) and capability. NIST conclude that this complexity implies that:

1) Failures in such systems can emerge from event sequences that are difficult to predict; and

2) The consequences of those failures, which typically require substantial time to diagnose and repair, can prove quite costly.

These factors, along with a number of high profile failures in Cloud computing systems, led NIST to identify the need to:

- formulate and publish best practices on achieving reliability;
- develop consensus on a process to measure and report industry-wide cloud reliability information;
- develop methods for measurement and monitoring to predict onset of catastrophic failure in cloud systems; and
- investigate tools to identify failure vulnerabilities in designs and deployments.

7.8 Chapter conclusion – large organisations will need to put in place a framework of standards and policies to ensure coherent and optimal use of Cloud computing services

The majority of public sector ICT costs relate to the provision of services to citizens, and this in turn involves many hundreds of relatively complex business services. Examples include “apply for a driving test” and “claim state pension”. The current ICT deployment model is to design the ICT enablers for such processes independently, and while all have some unique business logic, the majority include many common elements. (eg: “authenticate citizen”, “capture data”, “produce secure document”, “collect payment” and “make payment”). We identified the potential for improved outcomes and substantial savings by moving to a model where each of the common services is developed through a managed process, with two or three pan-government sources of supply of each. Such services could then be described in the catalogue, and made available for integration into the business specific processes of each organisation. This ambition is highly aligned with the principles of Service Orientated Architecture (SoA), with Cloud computing providing an attractive hosting and delivery model that readily allows SoA based services to be shared across multiple organisations.

8.0 Information Assurance considerations

This chapter draws on both the G Cloud Programme's Information Assurance Workstrand Report [25] that was issued in May 2010, and on subsequent developments through to September 2012.

8.1 Context

We found that the transition to Cloud computing services brings upside and downside risks from the Information Assurance perspective [25]. The downside risks include there being less, if any, control over changes made by the Cloud computing provider. Additionally the concept of using virtualisation technology to support multiple organisations and their information on the same physical device is relatively new and is not regarded as highly secure, and there may be still security vulnerabilities (for example in various hypervisors) that have not yet been discovered. There is also the reality that some Cloud computing providers prioritise features and early delivery to the market over and above exhaustive information security validation.

The potential upsides (from the Information Assurance perspective) of using shared Cloud computing services include that overall, large organisations should need to assure fewer services and thus increased assurance effort can be expended on each. Some risks may also be mitigated by the "superiority of numbers" advantage inherent in large-scale cloud provision; for example an industrial scale cloud provider may be able to withstand a multi gigabyte per second attack from a botnet that would overwhelm a conventional datacentre.

While the core information assurance risk areas of loss of confidentiality, integrity and availability remain unchanged [73], the global nature of some cloud service providers means that users often do not have control over where data resides. With many Cloud computing services data will quite possibly be held "at rest" or transition "in flight" outside national borders, for example UK "owned" data may be in the US, Asia or Eastern Europe. This may bring new risks such as personal being vetted to different levels, potential interference by overseas governments and unintentional breach of legislation that restricts where data can be held.

Given the proliferation of Cloud computing services the overhead of assuring each service individually can be prohibitive, and the concept of centralised pre-accreditation of core services has the potential to bring economies of scale as well as increase business agility. However,

before each deployment organisations will additionally need to consider the specific context of the service, the inherent information risks and the needs of the user community. This will need to be done on a case by case, organisation by organisation basis. There is also the need to consider the likelihood of there being sophisticated hostile third parties with sufficient interest in the information held to make a malicious breach a serious possibility.

Governments in the US and UK have introduced new information assurance frameworks [48] which are in part intended to remove some of the barriers to delivering services to citizens via the Internet, including the use of Cloud computing services. These approaches recognize that good commercial encryption and security technology is now suitable for much public sector data and services.

8.2 Key information assurance focus areas in a Cloud computing context

Amongst the areas to consider are:

- user and employee access control,
- protective monitoring,
- forensic readiness (collection of digital evidence),
- clarity on roles and responsibilities,
- having a security incident management policy,
- organisational standards for data encryption, both “at rest “and “in-flight”, and
- a sanitisation policy to ensure that data is securely removed when use of cloud service ceases.

Organisations will need to consider their information risk appetite, and put into place processes to ensure that this is addressed through the selection and usage strategy of Cloud computing services [73]. Given the lack of control over providers, organisations may wish to consider either appointing a broker responsible for mitigating security risks, or using combinations of cloud services in a way that mitigates the risk presented by any single provider, for example by encrypting data before transferring to the cloud provider, and ensuring that services can be sustained even where an individual cloud provider fails.

Achieving secure use of Cloud computing services for mission-critical processes requires investment in capability, service design, monitoring and management.

8.3 The criticality of "trust"

Establishing trust in cloud vendors is essential [74]. Current software technology does not provide guaranteed protection that data handled by a cloud provider will not be subject to unauthorized release or amendment. While this issue exists with the current outsourcing providers, the customer supplier relationship in those cases is much closer, and the degree of assurance provided is therefore greater. Additionally, in a Cloud computing context, there are likely to be increased risks both from other organisations and individuals who are using the same Cloud computing service, and from third parties making unauthorised accesses via the Internet.

The inherent risks include:

- System administrators may abuse their privileged access rights for unauthorised access and sharing of information.
- Rogue developers may build in malicious software implants into applications that, for example, could send data to other organisations.
- The increasing complexity and diversity of the supply base (resulting from the "multivendor nature") of cloud services makes it harder to manage risk, and to identify sources of failure if a loss occurs.
- Other users of the Cloud computing service may breach built-in virtualisation/hypervisor protections

8.4 Desired information assurance outcomes

The challenge from the information assurance perspective is how to manage the inherent risks of Cloud computing in a way that does not inhibit the progress that can be made with the achievement of business objectives.

Indeed, as explained above, a move to Cloud computing has the potential to enable the realisation of improved information assurance outcomes. At the same time this concentration of assets increases the threat risks; for example if a malicious party is successful in compromising a shared Cloud computing service, there is potentially access to a much wider range of information from many organisations.

Potentially, the information assurance regime associated with Cloud computing can become highly complex to deliver, and thus expensive (requiring lots of resource) and potentially complex to understand (and thus hard to manage).

Prerequisites therefore for the secure use of Cloud computing across a large organisation will be ensuring that there is a common business view of all the information assurance outcomes that need to be achieved, and clear agreement on the priority area(s) that should be addressed first. Mechanisms for establishing trust and a common approach across organisational boundaries will also be needed.

8.5 Information assurance objectives

Information assurance regimes typically seek to manage three main categories of risk [70]:

- loss of confidentiality of information that is private to the organisation, or which contains personal details of customers/citizens. The risk is that if information is in some way compromised, and thus becomes available to others, then inappropriately obtained information can be used to embarrass, threaten or defraud the rightful owner.
- Compromise of integrity, where information is changed by an unauthorised party potentially with the intention of causing harm or loss to the information owner. For example cases have been widely publicised where fraudulent parties have illicitly accessed online banking accounts, initiating or changing details of payments to steal money from the account holder.
- Impaired availability. Organisations are highly dependent on their information-based services, and in some cases have extremely limited fallback options. The risks can include reputational damage that may threaten future existence. Some organisations using Cloud computing services have suffered availability issues; for example customers of Amazon Web Services have reported lost data when individual disk drives fail, where customers have not adhered to AWS guidance on achieving resilience through splitting data across multiple “availability zones“ [60].

8.6 How do Cloud computing information assurance risks arise – What are the points of vulnerability?

There are multiple potential sources of potential compromise of information security; these can be categorised as originating with people, processes or technology. Some examples are provided below:

People

- Human error, eg failure to test fully, or deployment and configuration errors that inadvertently make private data available inappropriately.
- "Social engineering" attacks, e.g. bribing a system administrator who works at a Cloud computing provider to use the highly privileged access rights required for the job to steal or compromise information for the benefit of unauthorised parties.
- Attacks by organised crime or hostile countries. Parties who have access to extensive resource and technical capability will be able to compromise controls that may be perfectly adequate in other cases.
- User behaviour;- whatever controls are implemented at the "system" level, there can be problems with careless or abusive behaviour by system users, for example inadvertently leaving confidential information in public places.

Process

- Insecure automated registration procedures that allow individuals to assume another's identity when registering for a service.

Technology

- Design flaws in infrastructure and software
- Malicious implants in code
- Trojan and virus attacks on systems that result in data being sent to unauthorised third parties.
- Exploitation of what may be latent exposures in software by "customers" of the Cloud computing service, disrupting data or services belonging to other users.

8.7 Mitigation of conventional information assurance risks

In the UK, public sector organisations are obliged to adhere to the government's "Security Policy Framework"; this mandates an approach for managing information risks based on establishing the level of protection that is necessary taking into account both the consequences of loss of confidentiality, integrity and availability, and the likelihood of compromise occurring based on an assessment of "threat actors". The assessment is then used to determine the level of protection required, with protection levels being implemented through a combination of technical, personnel and procedural rules.

At present, each organisation assesses information risks individually. The process typically starts with the Chief Executive of the organisation appointing a "Senior Information Risk Owner" (SIRO), who will typically be a board member. The SIRO is responsible for assessing and securing board agreement to the "information risk appetite" of the organisation: this may differ for various categories of information and represents the trade off the organisation is prepared to make between with the costs and constraints of "maximum protection" versus the ease of use and innovation benefits that can come from an open approach to sharing information.

In the above context, the SIRO will then determine the information assurance requirements for the organisation's use of information;- for computer based information systems this will involve setting for example encryption levels, the levels of protection needed and vetting of staff required at the data centre, the vetting levels required of staff using the information system, and the procedural controls controlling access (e.g. who can authorise users to access the service, what categories of users are permitted, what audit facilities are needed etc?). Typically standard templates will be developed for the mainstream requirements of each organisation, e.g. published information (which while it may not be confidential still has an integrity and availability requirement), customer facing processes, with higher requirements for some specialist systems, (for example those implemented for security or fraud prevention purposes).

8.8 Mitigation of Cloud computing related information assurance risks

The G Cloud Information Assurance work strand was established in recognition that some changes to the approach to Information Assurance will be needed if Cloud computing services are to be adopted. In particular one of the principles of Cloud computing is to "use the service as is"; to get the economies of scale it is normal for all users of the service to be on a common

software release. In this context it is not practical for each organisational SIRO to request specific ad hoc security enhancements;- not least as implementing these could undermine the security basis (and thus the confidence) that existing users have in a service.

We identified that the key information assurance objectives need to be satisfied in the Cloud computing context are:

- Compliance: ensuring that cloud-based services and infrastructure operate within the requirements of applicable laws and policies.
- To detect and deter any unlawful activity.
- Risk management: ensure that risks are identified and managed.
- Reporting and continuous improvement: ensure that service management teams have a ongoing source of information on performance of specific cloud-based services as part of the "plan do check act" cycle of continuous improvement.
- Situational awareness: ensure that business and system monitoring teams have real-time information on the status of cloud-based services, enabling security incidents to be detected and remediated.
- Enabling accountability: ensure that the services and infrastructure are used within the parameters defined by the businesses.
- Network defence: Ensure the service can work with security countermeasures to enable a "defence in depth" approach, facilitating an automated response to threats to business services. (NB: Further information on the "defence in depth" approach is provided in Section 8.14)
- Service defence (distinct from network defence): given that most attacks are above the network layer, ensure that application level protection is in place, for example firewalls (e.g. XML and database), proxy servers and database reporting protections.

8.9 Information assurance related risks

The transition to Cloud computing services introduces a number of risks from the information assurance perspective. These include:

- Virtualisation and other systems software technologies do not today tend to have the capability or maturity to guarantee that information needing higher levels of protection will not become accessible to organisations with lower levels of security clearance who are sharing the same physical device.

- When using Cloud computing services, business applications, and arguably some forms of data (e.g. reference data) are no longer 100% attributable to a particular organisational entity.
- There will be new challenges in assessing the implications of aggregation and the separation of data within and between providers, both at the data centre level and on an enterprise basis.
- Cloud computing disaster recovery and backup facilities will be shared with other organisations. The guarantee from the Cloud computing provider may be a pure financial guarantee (i.e. in the event of a failure we will provide you with a refund'), rather than a genuine capability based guarantee that is underpinned by engineering capability and built-in redundancy across the Cloud computing providers' system resources.
- There may be unintended consequences at the "group" or "pan government" levels where multiple member organisations use cloud services independently, for example unintended excessive dependence on a small number of providers of communications circuits that could converge at a critical pinch points; e.g. transatlantic circuits to the UK.
- If an organisation becomes over dependent on a small number of cloud service providers, particularly those providing "software as a service", there is a risk that a rogue cloud provider could seek to manipulate its customers, e.g. by charging excessive prices, or by abusing data.

8.10 Mitigating information assurance related risks

It may be possible to mitigate some of the above risks by creating the "business services" required by the end customer organisation from a combination of cloud services in a way that provides protection (at the service and information levels) from the loss or compromise of any individual provider. For example by ensuring that all data is always held on at least two "infrastructure as a service providers", and by ensuring that there is always a fallback in the event that the customer case management or corporate e-mail systems fail.

Clearly, providing this type of resilience requires extensive analysis that will increase the costs for an individual organisation to deliver business critical services using Cloud computing providers. At the same time, for many organisations the business risk of not progressing such contingencies will be unacceptable.

Successful mitigation of these types of risks requires both detailed knowledge of the characteristics of individual cloud service providers, and the ability to build services that use (and thus effectively integrate) multiple providers.

While for many organisations it will not be economic to build the necessary capabilities and relationships in-house, the option of achieving these outcomes through engaging a "Cloud services broker" may still enable efficient and timely use of Cloud computing services.

8.11 Organisational framework for achieving secure use of cloud services.

We concluded in 2010 that the main elements of the information assurance model for use of Cloud computing services should comprise the following:

- The establishment of a senior group of business leaders who set the "information risk appetite" that will apply on a pan organisational basis.
- The creation of a pan government accreditor, who will conduct assurance of cloud services to validate if they comply, generically, with the predetermined "information risk appetite"
- Training in Cloud computing for organisational SIROs responsible for data that needs to be protected, setting out how SIROs can continue to have responsibility for accreditation of their organisation's data when using Cloud computing services that are shared with others.
- Initiation of common standards and approaches for:
    - user and employee access control.
    - protective monitoring (to be done at three levels comprising:
        - service providers undertaking routine collection and analysis of accounting and usage information.
        - cross provider analysis to identify any wider issues across providers.
        - schema wide "counter fraud" analytics to identify patterns of fraud, and to notify providers).
    - a forensic readiness strategy, providing the ability to collect, preserve, protect and analyse digital evidence, to a standard where this can be used in a legal context, for example in a court or tribunal.
    - a tiered approach to security management, with clarity on the role of the cloud provider, the pan government accreditor and the SIRO.

- a security incident management policy, to put in place the operational framework needed to respond to incidents with cloud providers as they occur, building on the procedures that exist within large organisations today, recognising that in future incidents will have impact across multiple organisations.
- A sanitisation policy, to determine what "cleanup" should be done on shared infrastructure after use by a particular organisation. This is needed to ensure that images of data are properly and routinely cleaned from memory, caching devices etc.
- an encryption policy, to put in place common encryption standards for "data at rest" and "data in flight".
- a common assurance approach, to determine what needs to be done to accredit suppliers, facilities, services (and where shared with other users) potentially other users. (NB: there also need to be clear criteria for "decertification").

8.12 Strawman Information Risk Management Roadmap

Based on the above, we identified a possible high level "strawman roadmap" for organisations wishing to adopt the use of Cloud computing services for sensitive information, as follows:

I. Determine the starting point. What are the shared characteristics of the datasets and services for which the organisation can get most initial value through the deployment of Cloud computing services?

II. Agree the information risk appetite that applies across these datasets, establishing a senior business decision group for this purpose if a suitable forum does not currently exist.

III. Establish the organisational entities needed, including the "pan organisation accreditor" and the "business unit's Senior Information Risk Owner".

IV. Determine to what extent public Cloud computing services can address each organisation's information and risk appetite constraints, and consider private services only where there are gaps in either information assurance requirements, or in functionality.

V. Consider what the approach to accreditation will be, and initiate a programme to select providers that best fit the business need, prior to putting formal accreditation in place.

VI. Determine what shared infrastructure is needed to support the Cloud computing usage model, for example this may include:

- Defining a trust model [9].
- A common user and employee identity management and role-based access control (RBAC) service.
- A portal providing a "directory of services", together with their accreditation status, user rating and price.

8.13 Loss of service risks

As covered in sections 5.6c and 7.7.1, NIST has observed that using Cloud computing services potentially exposes user organisations to new risks, in that Cloud computing systems are complex and can be of enormous scale. As a result failures can emerge from events that are difficult to predict, and where this occurs the consequences can be significant, with substantial time required to diagnose and repair. In designing the technical approach for using cloud services organisations need to be conscious of these risks, which in part can be mitigated by using a range of cloud services, avoiding complete dependency on any single provider for a "business critical" service or data.

8.14 Defence 'in depth' approach

Organisations will need to consider their information risk appetite, and put into place processes to ensure that this is taken into account in setting the strategy for the selection and use of Cloud computing services. Adoption of the defence in depth approach (depicted in figure 4 below) requires consideration of security at multiple levels, for example potentially including the encryption or fragmentation of data where it is not possible to establish full trust in particular providers.

We propose to adopt a generic multi-level 'defence in depth' approach as shown in Figure 4 (reproduced from the Information Assurance work strand report [25]).

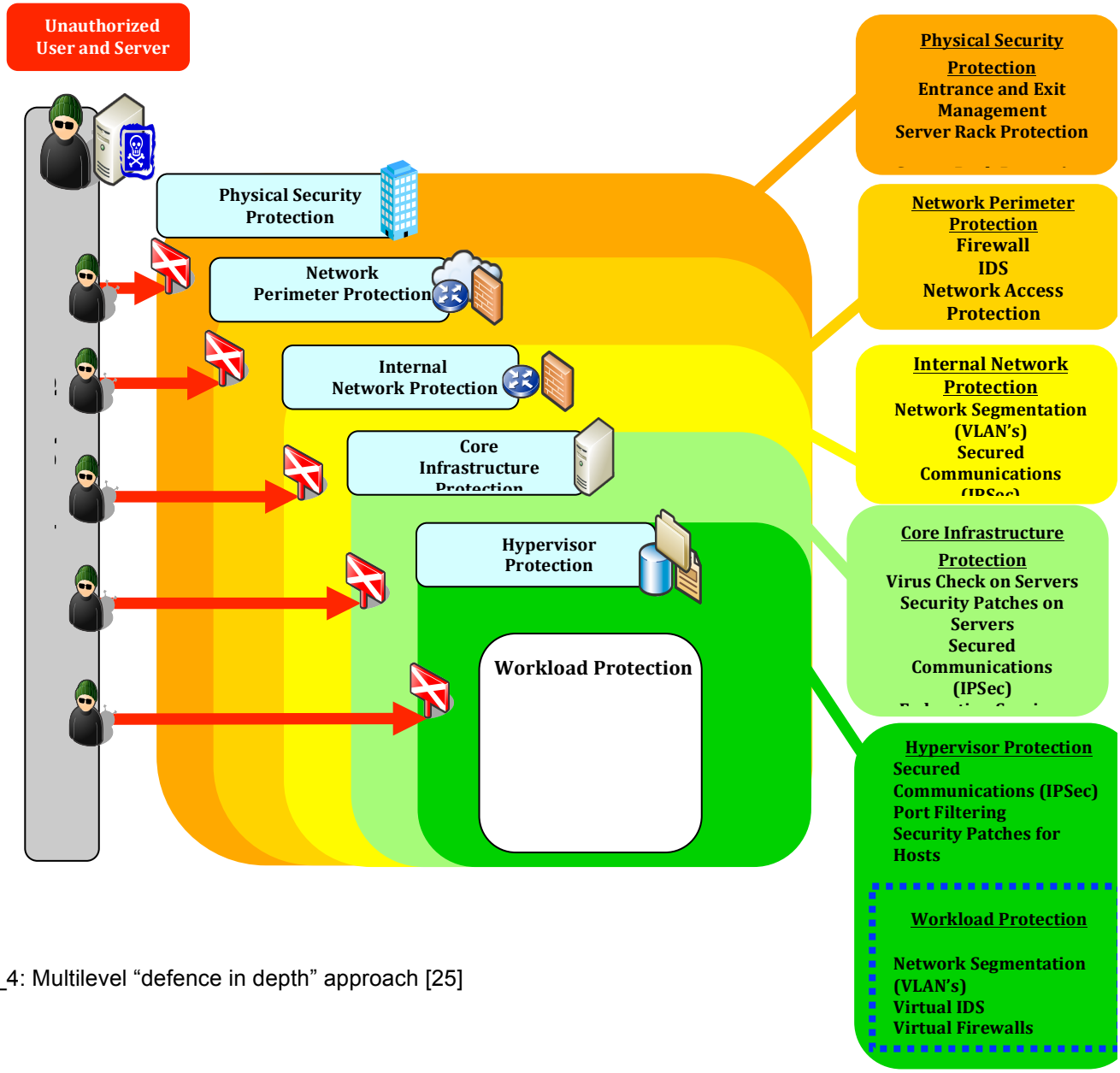


Figure_4: Multilevel "defence in depth" approach [25]

8.15 Potential role of Cloud Services Brokers and Service Orientated Architecture

Given the lack of control over providers, organisations may wish to consider appointing a broker responsible for mitigating security risks (as described in section 8.11), and using combinations of

cloud services in a way that mitigates the risk presented by any single provider, for example by encrypting data before transferring to the cloud provider, and ensuring that business processes can be sustained even where an individual cloud provider fails. This will particularly be the case when using public cloud services under standard contracts, which often give the provider the right to change the contractual terms simply by notifying consumers. This can present real risks:- for example in December 2012 Instagram (a consumer focused photo sharing website) announced a change in terms and conditions that (until revoked following public protest) would have given the supplier the rights to sell and retain revenue generated from selling photographs users had posted to the site.

The service orientated architecture concept is relevant to securing Cloud computing services. There is potential for "Cloud computing security service providers" to emerge, providing tools to monitor and audit the performance and behaviour of Cloud computing services. Achieving this would be considerably aided through agreement on standard interfaces for such security and audit purposes.

Achieving secure use of Cloud computing services for mission-critical processes requires investment in Information Assurance capability [75], and in setting standards and policies for secure service design, monitoring and management.

8.16 Rationalisation of government information assurance schema

For many years UK government has operated a six level schema for information classification;

- Unclassified
- Protect
- Restricted
- Confidential
- Secret
- Top-secret

While standard templates are provided from the centre, inevitably different organisations have different interpretations of what information should be categorised at each level, and the exact approach to be taken. One consequence of this is a lack of trust of information assurance accreditations that have been provided by other organisations;- today checks will typically be

redone even where the intent is to purchase an identical service from the same supplier, with the potential consequences of requests for suppliers to provide additional procedural or technical controls, which fragments delivery and adds to cost.

The UK government announced in 2013 that it would introduce a new information protection framework. The new scheme consolidates (from six) to three tiers of technical protection which in part is intended to remove some of the barriers to delivering services digitally to citizens, including the use of Cloud computing services. This approach recognises that good commercial encryption and security technology is now suitable for much public sector data and services. This involves firstly introducing a new classification level (Official) that will apply to the data needed for the majority of its services, and secondly to define the technical protection needed at this level so that it can be provided by good commercially available products, rather than needing bespoke development. Special measures (technical and other) will remain in place for information that is classified as "secret" or higher.

The new "Official" classification level will be introduced in 2014. It will be used for the majority of data that underpins citizen facing services; which is where the majority of transactions and thus ICT costs, lies.

This represents a substantial step forward in implementing the simplified information assurance regime needed for the efficient use of Cloud computing services; firstly as it provides focus for professionals across government to use a single approach for the majority of services. Secondly it also provides focus for the supplier community, providing "a critical mass" of potential business that justifies investing in providing "official" level services, and making these available via CloudStore so that they can be called down on an "off-the-shelf "basis as and when required.

8.17 Chapter conclusion – Managing the information assurance risks in using Cloud computing services

We found that the transition to Cloud computing services potentially brings benefits as well as risks from the Information Assurance perspective [8]. The risks include there being less, if any, control over changes made by the Cloud computing provider. Additionally the concept of using virtualisation technology to support multiple organisations and their information on the same physical device is relatively new and is not regarded as highly secure, and there may be still security vulnerabilities that have not yet been discovered. There is also the reality that some

Cloud computing providers prioritise features and early delivery to the market over and above exhaustive information security validation.

The potential benefits (from the Information Assurance perspective) of using shared Cloud computing services include that the organisation overall needs to assure fewer services and thus increased assurance effort can be expended on each.

While the core risk information assurance areas of loss of confidentiality, integrity and availability remain unchanged, the global nature of some cloud service providers means there is less control over where data resides. With many services data will quite possibly end up outside national borders, potentially including countries that may be regarded as “higher risk”. This in turn may bring new risks such as personal being vetted to different levels, potential interference by overseas governments and the possibility of inadvertent breach of legislation that restricts where data can be held.

We considered that the proliferation of Cloud computing services means the overhead of assessing candidate services individually can be prohibitive. Hence the concept of centralised pre-accreditation of services by a broker has the potential to bring economies of scale. However, before each deployment organisations will additionally need to consider the specific context of the service, the inherent information risks and the needs of the user community. This will need to be done on a case-by-case, organisation by organisation basis.

When selecting Cloud computing services organisations need to consider a range of information assurance issues including:

- user and employee access control,
- protective monitoring,
- forensic readiness (collection of digital evidence),
- clarity on roles and responsibilities,
- having a security incident management policy,
- organisational standards for data encryption, both “at rest “and “in-flight”, and
- a sanitisation policy to ensure that data is securely removed when use of cloud service ceases.

We advocate the adoption of a ‘defence in depth approach’;- this involves consideration of security at multiple levels, potentially including the encryption or fragmentation of data where it is

not possible to establish full trust in particular providers. Organisations will need to consider their information risk appetite, and put into place processes to ensure that this is taken into account when setting the strategy for the selection and use of Cloud computing services.

9.0 Service Management

This chapter draws on both the G Cloud Programme's Service Management Workstrand Report [27] that was issued in May 2010, and on subsequent work.

9.1 Cloud computing ICT Service Management:- summary conclusions

Service management using Cloud computing services presents new challenges; as in other areas there is reduced control over providers' approaches. Further the commoditised "as is" nature of services means that it will often be necessary to use two or more together to achieve a particular business process outcome. Given the limited control of any particular customer, it will usually not be possible to understand the engineering detail how the service has been constructed, and thus also impossible to model fully how the service will perform under various extreme scenarios. It will be necessary therefore to rely on commitments and assurances made by the Cloud computing vendor. Potentially, these can be verified by independent auditors [63].

For the foreseeable future establishing trust in Cloud computing suppliers will therefore be essential. In the longer term these risks may be mitigated should standards and markets transparency develop to the point where "instantaneous transfer" to an alternative service becomes possible.

In the near-term organisations will need to ensure that there is a framework for managing Cloud computing services, and that this is taken into account when determining the approaches for sourcing, governance, procurement and management of Cloud computing services.

Where a cloud service is being used together with internal services, or where several cloud services are being used together, there will be a need for a "service integrator" to be accountable for achieving a predictable end to end service outcome that builds on the SLAs of each service provider.

Standards for service management would be of benefit to service integrators in predicting, measuring and sustaining service outcomes. Currently there is a lack of maturity in this area; while the IT infrastructure library (ITIL) provides a possible framework, it was specified with conventional ICT delivery in mind, and is currently somewhat inconsistently deployed to varying levels by organisations.

This implies therefore that consuming organisations will need to do significant work with each cloud provider before adopting services for high priority business processes.

The cost of doing so for individual organisations will be significant, and it may therefore be preferable to contract out this role to a third party organisation. Phase 2 of the G Cloud Programme identified such a role, that was provisionally named the "integrated services manager". Subsequently industry analysts have identified this as one of the roles that could be performed by a Cloud services broker.

9.1.1 Key activities

We considered the key activities to be performed by each participant in the service management domain to be as summarised in Figure 5 below (This is reproduced from the Service Management workstrand report [27]):

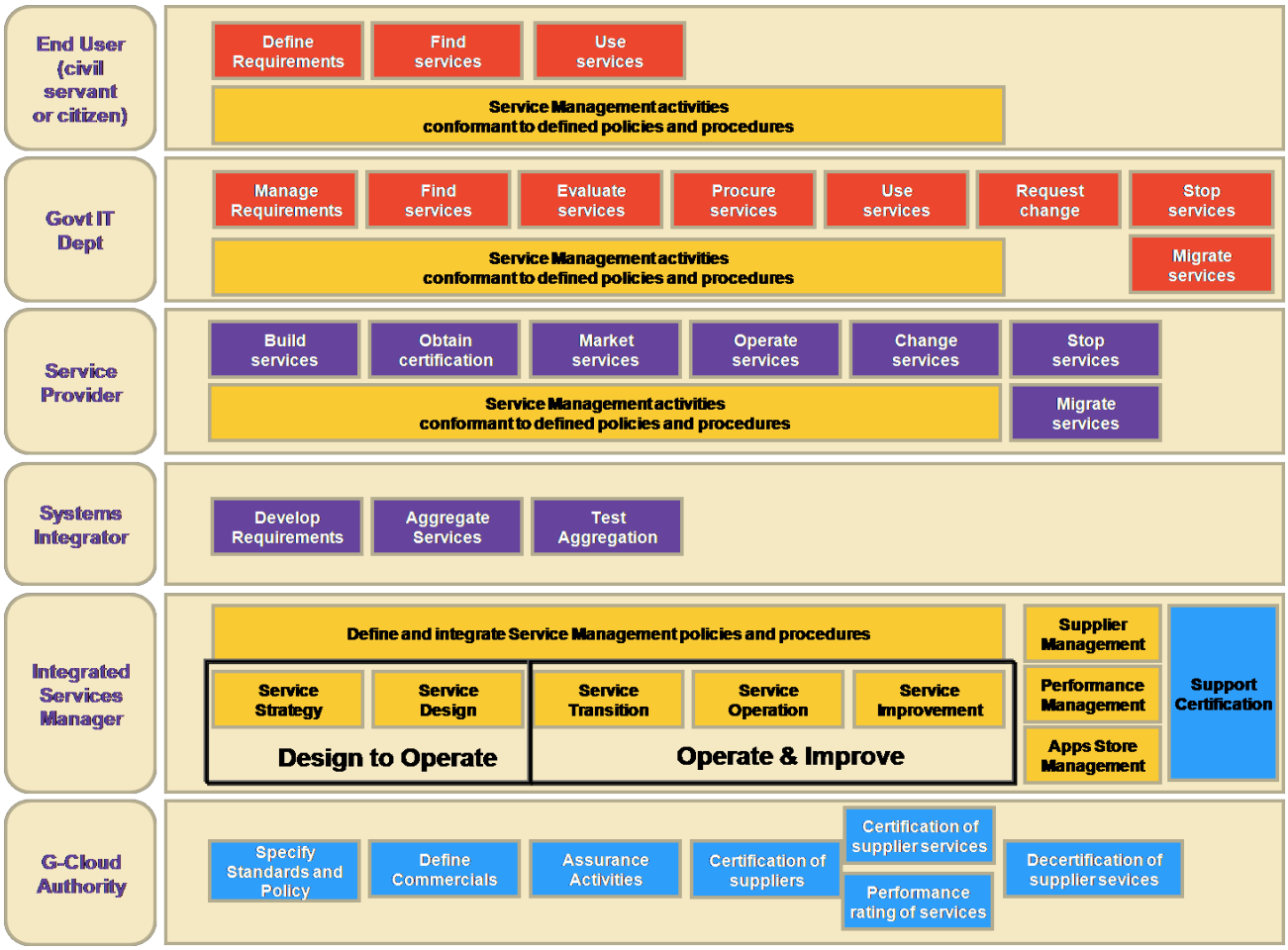


Figure 5: Service management activities involved in Cloud computing [27]

Establishing trust in Cloud computing suppliers will be essential. Cloud Services brokers have a key role to play in performing the services shown at the base of figure 5, i.e. those designated for the G Cloud Authority [11] [58].

9.1.2 *Framework for service management of Cloud computing services*

In the near-term organisations will need to select or design a service framework for managing Cloud computing services. As depicted in the diagram below (which is reproduced from the Service Management workstrand report [27]):, such frameworks will need to recognise that the more sophisticated and embedded in the business a service is, the greater the range of service management activities that will be needed:

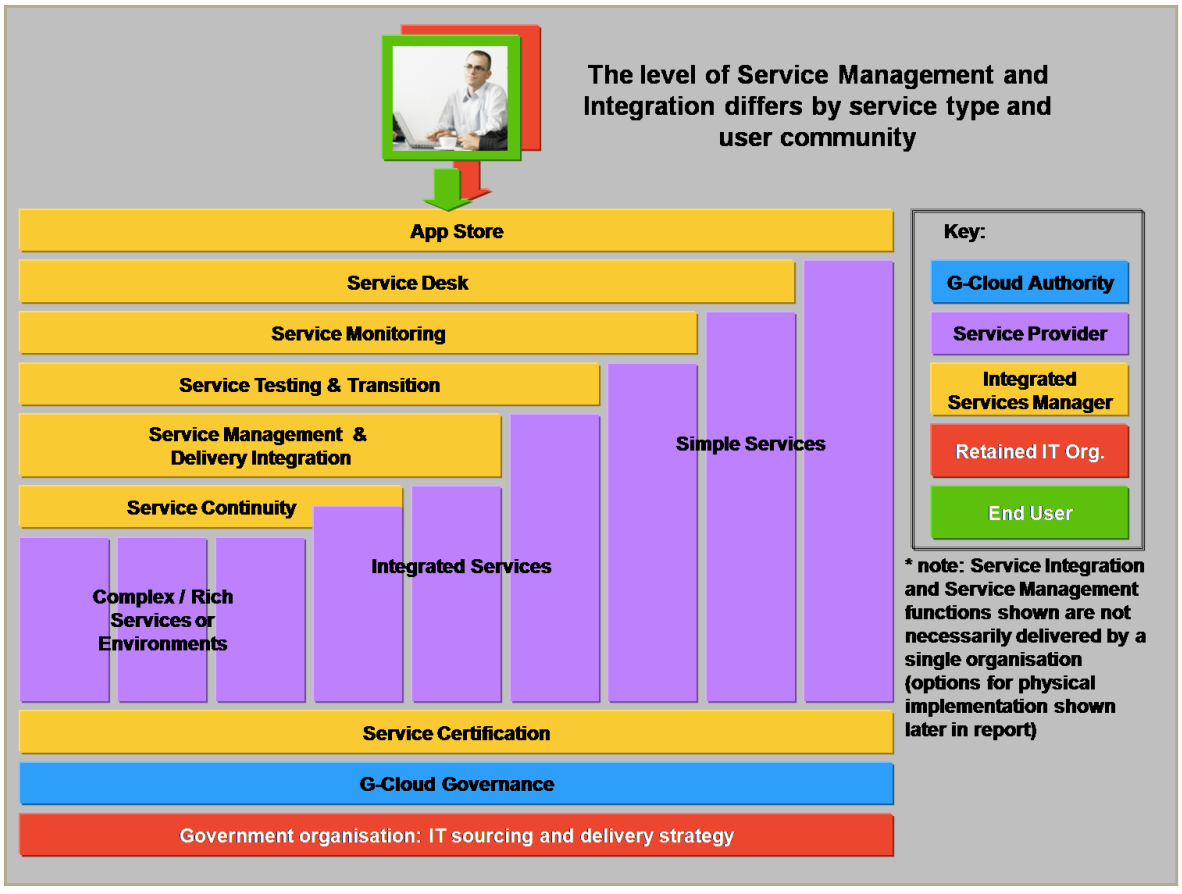


Figure 6: More intensive service management engagement is needed for complex services [27]

We identified that the future ICT enablement for business processes will often use a combination of internal services (similar to those typically used today) and new externally sourced Cloud

computing services. As existing service management toolsets are typically only designed to support the management of internal services, we concluded that new service management tooling will be required; for example so that the helpdesk can maintain a "service dashboard" providing a holistic view of the information services their organisation is using (internal and external), including those based on Cloud computing services.

For many organisations the costs of commissioning in depth due diligence with multiple Cloud computing suppliers will be prohibitive, and it may therefore be preferable to contract out this role to a third party organisation.

The implication therefore is that consuming organisations will need to ensure that significant validation work has been undertaken with each cloud provider before adopting services for processes that are business critical. Again market adoption of Cloud computing services will be eased if Cloud service brokerages have invested in providing these assurance services, enabling consuming organisations to establish trust at a lower cost than would be incurred through entirely internal assurance activities.

9.1.3 Phased approach to building service management capability

As in other areas it is clear that there are there are complex challenges to address, and again a phased approach seems inevitable; starting with relatively straightforward use of Cloud computing services in less business critical areas, in anticipation that suitable "integrated service providers" will emerge from the ICT industry over time.

9.2 ICT Service management challenges

Service management in a Cloud computing environment is more complex than for a traditional "on premise" model for two main reasons [76]:

- Firstly, in a Cloud computing environment an organisation may well be sourcing ICT services for a single business process from several different suppliers. If the process fails or performance decays it will be necessary both to quickly identify which service provider is causing the problem, and to be able to manage any issues that span across multiple service providers.

- Secondly, the providers of Cloud computing services have to take into account the requirements of potentially many thousands of customers. A key assumption of Cloud computing providers is that a single software version supports many thousands or even millions of users. In this environment, is rarely practical to accommodate a single customer's request for change or enhancements, in contrast to the "on premise" world where the software based services are provided primarily for a single customer, whose future requests and enhancement roadmap are important to the supplier as it represents an ongoing source of further income.

The additional complexity outlined above further reinforces the need for effective ICT service management when using Cloud computing services in a "business critical" context.

We found that the desired outcomes are:

- the service management framework enables streamlined purchasing of services that can be integrated to together provide a business process outcome.
- Purchasers of services have genuine choice, in that services can be compared on defined criteria (with consistent interpretation) covering attributes such as support, availability, response times etc.
- Service performance measures are aligned to business process measures, or business process outcomes.

9.3 Integrated service management model

Use of Cloud computing services in a corporate ICT context remains a relatively recent innovation, and for this reason there are not today recognised ICT service management models that represent accepted "industry best practice" in these areas. Specifically, there is not a recognised service management model setting out how to use an externally provided Cloud computing service in conjunction with in-house "on premise" (legacy) services. Neither is this in place for the more complex (and potentially greater business adding value) scenario where combinations of public, community and private cloud services are together used to provide the enablement for a business process.

While there are a number of approaches an organisation could adopt to build its own integrated service management model for managing the operational relationship with cloud service

providers, it will often be more beneficial to outsource this activity to a specialist “cloud service broker”.

We identified that amongst the areas that organisations wishing to make widespread use of Cloud computing services will need to consider are:

- ensuring there is an effective service management model that can be applied across vendors.
- the sourcing approach for Cloud computing services.
- the overall governance model, setting out clear roles, accountabilities and responsibilities.
- the procurement model.
- how to measure performance and return on investment.

We concluded that the success of the G Cloud ICT service management model would to a significant extent be assessed on the basis of establishing trust;- specifically has the service management approach succeeded in establishing trust in the ability of organisations using cloud services to achieve predictable and secure business outcomes, without needing to directly control each “link in the chain”?

9.4 Framework for ICT service management when using Cloud computing services.

The goal of ICT service management is to ensure that, on a day-to-day basis, the ICT services provided meet desired business outcomes in terms of quality, service operations, customer satisfaction and business alignment [76]. This involves both ensuring that services are “fit for purpose” in the context of achieving their intended business outcomes, and that there is sustained pressure to progressively reduce costs.

Before selecting Cloud computing services, business level service outcome specifications should first be defined given that in most cases, Cloud computing services do not by themselves meet the true end user/business need. As a minimum, there must be access to the right data, held with appropriate levels of protection/security. Additional integration will be needed in many situations, such as with user authentication services. Hence while it will be necessary to have an understanding of the characteristics and the sources of the technical services that are delivered by Cloud computing providers, this will not be sufficient by itself. The starting point needs to be

the business context, with the end to end characteristics of the business process understood, and a clear definition and delineation of the role of all computing services used in its delivery.

Within this context, we considered the "critical success factors" for using Cloud computing services, specifically the prerequisites for confidence and trust that these will reliably deliver the desired business outcomes. We concluded that these comprise:

- Use of Cloud computing services has been planned from the outset within a "design to operate, end to end" perspective.
- The role of "service integrator" has been defined, and clear measurable objectives for the desired service outcomes have been set (expressed in terms such as response times, availability, business continuity, service level agreements etc).
- The service integrator selects accredited services (that meet functional, non-functional, information assurance and commercial requirements), and using common service measures, integrates these together in a way to achieve a predictable end to end service outcome, with the contribution of each service provider known.
- There is a specified "roles and responsibilities" model so that all are clear on "who does what and when" and a coherent (and ideally common) support model is in place across all component cloud services.
- There is an overarching governance framework that enables all of the component ICT and support services to be jointly used to deliver the desired business outcome, and that there are standard measures and definitions at all levels, so that "apples with apples" comparisons can be made.

9.5 Risks

While it is relatively easy to define the objectives (as above), realising these in practice is challenging. Specifically, the desired focus of many ICT projects is on creating business logic [77] , rather than on creating the software and infrastructure environment needed for the business logic to run reliably. Within large organisations that build in-house ICT for on premise usage, there will typically be standards and common models for building the necessary software and services environment, which in turn means it is not necessary to revalidate details for every new application. We identified that a key risk of the transition to using Cloud computing services is that organisations will feel that they need to validate the system software architecture and the internal operational procedures of the cloud provider. This creates the risk that the costs of

discovery renders such usage prohibitively time-consuming and expensive, given that cloud providers do not routinely expose all the details of their services. Indeed it may not be possible to obtain clarity on specific attributes of services beyond that which is published on the supplier's website.

9.6 A possible "end state "service management model for using Cloud computing services in the large-scale organisation.

We developed a possible "end-stage" model to recognise the different roles and responsibilities of various participants in the "system" of organisations that is providing and using Cloud computing services. These include:

- the end-user.
- the purchasing organisation.
- the cloud service provider.
- the cloud services integrator.
- (potentially) the cloud services regulator.

Risks arise from many different sources, and range for example from possible employee abuse of privileges to loss of service due to damage to data centres in unstable countries. Hence before using cloud services for business critical use, purchasing organisations will wish to validate that the proposed providers of cloud services are reputable, and that they have the internal capabilities to ensure that continuity of business can be sustained. The questions that need to be addressed include:

- suppliers' financial stability.
- service management procedures used.
- staff training and vetting procedures.
- information assurance policies and compliance (to ensure confidentiality, integrity and availability of information assets).
- adherence to generic standards, e.g. data formatting (open standards?).
- use of a standard identity management schema.
- commercial policies.

It is again clear that the costs of performing the detailed assessments set out above on potential new cloud service providers will be significant, and will therefore be difficult to justify except where expected usage levels are very high.

9.7 A framework for cloud services integration.

ITIL is the most mature framework used for ICT service management [23]. It covers:

- service strategy
- service design
- service transition
- service operations
- continual service improvement

However, we determined that ITIL implementations differ significantly in interpretation between organisations, as do the elements of ITIL that have been implemented. Hence while it represents a good starting point for creation for management of a hybrid of cloud and internal services, further work is needed. It also does not recognise some of the new features of Cloud computing, for example that user organisations have less control (potentially substantially less) than in the traditional on premise environment. There are also broader issues to consider, such as the risk of major impact on the organisation at group level, in the event of the failure of a provider, should a number of business units or divisions all have selected the same cloud service independently.

9.8 Role of the cloud services broker.

We found that Cloud services brokerages can achieve economies of scale by conducting the necessary assessments on each provider once for all their clients. Provided that there is sufficient trust in the broker, the validated services can then be entrusted for use by multiple consuming organisations.

In addition to sharing the overheads of the costs of service validation, the cloud services broker can potentially enable other innovations too. For example the investments necessary to create an online cloud services catalogue with the auto provisioning and data migration tools discussed in Chapter 7 can be undertaken by the broker for the benefit of its (multiple) customers.

Cloud brokerage services could extend to include tools to help selection of the most appropriate and cost-effective combinations of cloud services to achieve specified business outcomes, with

the selection tools being aware of the potential interoperability of various cloud services with respect to the standards that each has implemented for data exchange, service management etc.

In summary, the activities undertaken by a cloud services broker could thus include:

- running an online "application" catalogue.
- providing configuration tools that allow selection of compatible services from within the catalogue, with "real-time" assessment of the end to end service performance that can be achieved from particular combinations of services.
- providing a selection of optional add-on services, such as financial guarantees where the service fails, or physical backup supported by a robust engineered solution.
- providing cost comparisons, and aggregating purchasing volumes across so that the broker can negotiate better end-user pricing.
- building and configuring services, to include provision of connectors that help to integrate various cloud services, and the tools to migrate existing data into the cloud service.
- at the run and operate stage, creating an end to end service dashboard illustrating the status of the various Cloud computing services involved in underpinning a business process, and highlighting where services are impacted by operational problems, making clear what impact these are having on end-user business process outcomes.

Within the G Cloud programme, we envisaged that "stand-alone" cloud services could be requested and bought directly from the catalogue, but that where integration of two or more cloud services is required to deliver a business process outcome, then the broker (or integrated services manager) would provide the "joined up" service. In either case the broker needs to:

- provide and manage the catalogue, being clear on what services can readily be used with each other (perhaps the most important offering),
- integrate services where needed,
- operate the service desk,
- provide service continuity,
- offer support for test and transition,
- monitor service performance.

Once deployed, there will be new challenges in managing business processes that are comprised of multiple Cloud computing services. For example, if a provider suffers a problem how can the impact on the business be determined quickly? We considered that a possible

solution would be to develop a “service information monitor” to enable rapid analysis in the event of a failure of a provider or composite service, to ascertain which end-user organisations will be affected by the outage, and to what severity.

Hence again it may be more economically viable to subcontract the assurance of new cloud services to a specialist cloud services broker.

9.8.1 Cloud services “front-page”

Managing the bigger picture once multiple cloud services have been deployed will require a “real-time” dashboard or similar. Potentially, service management tools such as the “front page” and the “service information monitor” could be bought from the CloudStore. The G Cloud programme identified around 25 cloud management services that could potentially be offered and provisioned through CloudStore [26].

9.8.2 Organisational models to support the cloud services broker.

There are both market and regulatory approaches to establishing cloud service brokerages. The market approach would see openness and encouragement of organisations that are currently active in supporting the use of cloud services to extend their range of services, and to automate delivery of those that are used in high volumes to help drive down costs.

Alternatively, there could be a regulated approach to ensuring supply of such services, and this could be done on a number of bases; for example:

- a new central organisation is established to act as a cloud services broker on behalf of the organisation or community.
- large business units are mandated and licensed to act as cloud services brokers, providing services to other member organisations.
- business units with similar characteristics could be encouraged to work together, forming “business communities” and creating their own cloud services brokers.
- there could be an “light touch” approach allowing each organisation considerable autonomy for each member organisation to choose if, how, and when to deploy cloud services.

Overall, it appears likely that a market-driven approach will yield better results in the long-term, although the development of the industry may need to be stimulated by large organisations including governments supporting one of the “planned economy” models mentioned above, with the intent to subsequently transfer any cloud services brokerage organisation that is created into the private sector, once established.

9.9 Scope for a phased, multilevel approach to developing cloud service brokerages

Different levels of sophistication are needed for different cloud service usage scenarios.

9.9.1 Simple usage scenario

The simplest case will be where a single service is used in isolation to meet a business need. For example, in the Ministry of Justice, Huddle [5] (a cloud-based collaboration service) is being used to support a number of teams that have a need to share information. Even in this case however it was deemed not sensible to allow Huddle deployments to be completely independent of the broader ICT support structures. Hence Huddle has been integrated into the standard service management and commercial processes, so that for example price reductions can be tracked to ensure they come through as expected, and that if there is a service problem and the user calls the helpdesk, the agent taking the call knows how to validate the problem that’s been reported, and who to escalate to if it cannot be immediately addressed. These service management overlays add to the cost of using Cloud computing, reducing the savings from the “headline price”.

9.9.2 Possible intermediate step

We concluded that for the purchase of relatively simple services that are used in isolation, the services of a cloud services broker may not be necessary. For example if a service is being bought for collaboration with external parties, with access via the Internet, there is relatively little value that a cloud services broker can add, though arguably still some;- for example assistance with configuration, administration (eg billing) and aggregation of purchasing power.

In the case of more complex services though service integration will be required, i.e. an approach that will ensure an end to end business outcome will be achieved from using a

combination of services. This is discussed in the paper “Towards Secure Cloud Bursting, Brokerage and Aggregation” [78].

As an intermediate step, there are a number of organisations that assist with the selection, implementation and integration of cloud services. Today, these types of organisation primarily assist their clients with the selection and deployment of cloud services, utilising a range of tools including connectors to assist with legacy integration, and data migration tools. One of these organisations has advised that they typically find that 25% -- 50% of a client’s in-house ICT services can be readily migrated to cloud services, with current approaches tending to select different cloud platforms for each service migrated, with relatively little information exchange between services.

9.9.3 Longer term - a multilevel approach?

As the use of cloud services matures, it is likely that a number of different styles of management will be recognised as being necessary:

1. Business process level.

Complex business processes will consist of a combination of business services, some of which may be provided in-house, with others sourced from private, community or public cloud providers. At the business process level it is necessary to ensure end-to-end performance, reliability etc and that exceptions are handled in a way appropriate to “the business context”.

2. Business service level

Business services may be used in multiple business processes. For example a generic reusable capability, such as a document retrieval system, or a payment processing system can be deployed in a variety of contexts. Such business services will need operational management in their own right, i.e. to ensure that its performance, security, and capacity are kept in balance with demand. Business services may be deployed by “platform as a service” providers; others will be classified as “software as a service”.

3. Infrastructure is a service

Some business services may be based on Infrastructure as a Service platforms. The management challenges of Infrastructure as a Service are different again; but they are likely to include greater "hands-on" end user involvement in specifying physical and operational characteristics of the service, for example is a backup copy of the data held and where is it located, how can this be restored, and what service metrics are actively used?

9.10 Service Management roadmap for cloud services deployment.

As a starting point, the earliest delivery of benefits will be realised by a combination of:

- directly deploying "stand-alone" cloud services where they can meet an immediate need cost effectively, even if as a "point solution", and
- engaging specialist deployment partners to assess the scope for deploying existing public cloud services to help address more complex business problems, for example the replacement of existing ERP systems.

Once benefits have begun to be realised as above, the next step will be to engage a cloud services broker, their involvement can commence with the provision of configuration tools and studies on how more complex information services and business processes can be created. Such initiatives can then be piloted, and subsequently deployed. In such cases the cloud services broker may need to:

- create configuration and performance assessment tools,
- create data migration and integration services,
- provide assistance with commercial management of cloud suppliers, ie to drive down prices.
- provide helpdesk and service information, as well as
- actively contributing to service governance, seeking to influence the cloud provider's future direction to meet the business needs of the brokers' customers.

9.11 Chapter conclusion – Managing risks to ICT service continuity when using Cloud computing services

We found that Cloud computing presents new challenges for the ICT Service Management community. In contrast to the established 'on premise' model, those purchasing Cloud

computing services have no control over providers' approaches to ICT Service Management, and have to rely on 'good practice' being implemented. Further the commoditised "use as is" nature of Cloud computing services means that it will often be necessary to use two or more together to achieve a particular business process outcome.

Given the limited control of any particular customer, it will not usually be possible either to access the engineering detail how the service has been constructed, or to fully model how the service will perform under various extreme scenarios. It is therefore necessary to rely on commitments and assurances made by the Cloud computing vendor, with these being potentially verified by independent auditors.

Establishing trust in suppliers of Cloud computing services is therefore essential. In the longer term some aspects of these risks may be mitigated if regulation, standards and market transparency develop to the point where "instantaneous transfer" to an alternative service becomes possible. The implication therefore is that in the short to medium term consuming organisations will need to ensure that significant discovery and validation work has been with each cloud provider before adopting services for business critical processes.

Where a cloud service is being used together with internal services, or where several cloud services are being used together, there will be a need for a "service integrator" accountable for achieving a predictable end to end service outcome for business users. Methodologies will be required that build on the SLAs of each service provider. Standards for Service Management would be of benefit to service integrators in predicting, measuring and sustaining service outcomes. Currently there is a lack of maturity in this area; while the IT infrastructure library (ITIL) provides a possible framework, it was specified with conventional ICT delivery in mind, and is not consistently deployed across organisations.

In the near-term organisations will need to ensure that there is a framework for managing Cloud computing services, and that this is taken into account in developing the approach for sourcing, governance, procurement and measurement. This framework will need to recognise that the more sophisticated and embedded in the business a service is, the greater the range of service management activities that will be needed.

New service management tooling will also be required; for example so that the helpdesk can maintain a "service dashboard" providing a holistic view of the information services their

organisation is providing (internal and external), including those that include Cloud computing services.

10.0 Commercial and legal implications of using Cloud computing services

This chapter draws on both the G Cloud Programme's Commercial Workstrand Report [52] that was issued in May 2010, and on the author's subsequent experience.

10.1 Introduction: Market structure for Cloud computing services

In their book "Economics" [92], Begg, Fischer and Dornbusch set out the characteristics of market structure in the table that is reproduced below:

		Imperfect competition		
Characteristic	Perfect competition	Monopolistic competition	Oligopoly	Monopoly
Number of firms	Many	Many	Few	One
Ability to affect price	None	Limited	Some	Considerable
Entry barriers	None	None	Some	Complete
Example	Fruit stalls	Corner grocer	Cars	Post office

Table 1: Market structure (reproduced from "Economics" [92] by Begg, Fischer and Dornbusch)

Using the above table as the basis for assessing the market structure of Cloud computing providers, different characteristics apply to the main categories of Cloud computing providers, specifically:

a) Large integrated cloud providers demonstrate some of the characteristics of oligopoly. It is also relevant however that the newer entrants are in most cases displacing business from incumbents in more established areas of the IT industry. Indeed the newer entrants' ability to enter and disrupt the market of large scale enterprise ICT suppliers is founded on the scale and commoditization advantages that result from their success as large scale providers of consumer internet services. Viewed from this latter perspective this suggests that collectively even these large-scale providers do not have the full market power of an oligopoly, as winning new business is dependent on having a superior proposition to those of the established industry incumbents.

b) Software as a Service (SaaS) providers who build added value services running on one of the major integrated cloud platforms are arguably operating in a "monopolistic competition" environment [44]. Barriers to entry are relatively low, a great many organisations are competing to offer new services, and it is relatively easy to compare services on price versus both other cloud computing providers, and traditional IT supply options.
c) Likewise, some aspects of "monopolistic competition" are increasingly seen from local infrastructure service providers, for example Skyscape [35] and FCOS, who both leverage the Cisco, EMC and VMware alliance (VCE) commoditised cloud technology to offer a customized "infrastructure as a service capability" to meet UK public sector needs, differentiated by demonstrably meeting information assurance and data residency requirements.

From the buyer's perspective, it is important to recognise that there is not a "perfectly competitive market" [44] for Cloud computing services. Specifically while pursuing the benefits that are attainable, purchasers of Cloud computing services need to recognise risks at may inhibit realisation of these benefits such as lack of consistency of services, significant entry and exit barriers (ie costs), and potentially high transaction costs. This applies particularly where data migration is complex, or where users need to negotiate changes to standard "click to accept" contracts.

The commercial risks would be lower if an organisation's requirements could be met by genuinely commoditised services. This would provide choice, and thus the ability for users to switch to an alternative service if unsatisfied. Starting points for consideration of Cloud computing services may thus include business needs that potentially can be entirely addressed by the use of commodity services, for example website hosting, widely used applications such as e-mail and basic word processing, and development and test services. However even though these types of service are provided by many Cloud computing providers; services are far from identical, competition thus falls short of being 'perfect' and hence it is not possible to compare on price alone.

A more competitive marketplace for Cloud computing services may develop over time. Government could potentially help stimulate this by the sponsorship of standards that will apply across a large community group. Progress can potentially be accelerated if there is alignment

across a geographic area, for example through the standards being specified by the EU, US and some other governments [79].

10.2 Objectives for Cloud computing commercial framework

From the commercial perspective we identified that the framework for using Cloud computing services needs to ensure that:

- change is simple and easy to achieve.
- pricing is transparent and comparable.
- there is a standardised purchasing model.
- there is confidence that suppliers will meet minimum technical, commercial and Information Assurance standards through working within a common governance framework.
- buyers retain the choice of switching to alternative services (or combination of services), for example where the service initially selected ceases to be the most functional or price competitive over time.

It was also acknowledged that the creation of an enterprise cloud services marketplace needs to take place in parallel with a realignment of skills, culture and behavior across ICT practitioners. (This is elaborated in section 10.7.2).

From the perspective of commercial practitioners a phased approach to deploying Cloud computing services is again preferable, starting by building experience and confidence in use of relatively simple services in lower risk areas of business, building experience over time.

10.3 Core commercial principles for Cloud computing services

As discussed in earlier chapters, the main promises of Cloud computing include reduced costs and faster “time to deployment” for new business applications. Cloud computing providers’ ability to deliver these benefits is founded on the ability to deliver standardised ICT services at large-scale. This in turn is enabled by progress in the adoption of Internet standards, large-scale data centre provision, data centre automation and application of e-commerce business models to ICT services.

From the commercial perspective, this means that users of Cloud computing services:

- do not incur capital expenditure costs, as consumers do not own the ICT infrastructure.
- purchase on a "service" basis, paying only for what is used on either a subscription basis or a pay per use model.
- do not always need to understand the detail underpinning the provision of services
- have the ability to scale ICT capacity up or down far faster than with the traditional "on premise" approach. For example Amazon Web Services has been used to scale ICT capacity in near real-time in response to consumer demand resulting from advertising campaigns.

10.4 Ensuring ongoing competition in the marketplace for Cloud computing services?

Recognising that the market sector that comprises very large cloud computing suppliers displays some of the characteristics of oligopoly, a key consideration is how to manage the resulting risks to service consumers.

Oligopoly typically arises where there are a relatively small number of long term market participants who enjoy scale advantages, and who can thus generate large profits which in turn can sustain by significant ongoing investment . While oligopoly arguably brings some benefits to consumers (e.g. relative stability of suppliers and predictability of pricing), there are also significant disadvantages including [93]:

- Setting of prices may be advantageous for the firms, but prices may be set at a level that proves to be a great disadvantage for consumers.
- Creative ideas or plans of small businesses in the oligopolistic market fail to realize because they small businesses cannot overcome the control of major market players. Their realization is only possible when one of the major player adopts the ideas of a small business for its own use.
- Small businesses in an oligopolistic market fail to establish themselves as a brand because most of the market is captured by larger firms.
- With the presence of little competition, dominant companies may not think of improving their products.
- Firms cannot take independent decisions and always have to consider the views of other dominant players in the market.

- New firms cannot enter the market easily due to various barriers of entry.
- The micro-economic goal of fair wealth distribution is not fulfilled as maximum profit is made by major players only, and small players are left with little profits.

This prompts the questions firstly of whether it is appropriate, and secondly whether it is practical to seek to regulate the marketplace of suppliers of very large-scale cloud computing services.

In his paper "Competition policy in the information economy", Carl Shapiro [94] sets out six principles for firms competing in the information economy:

- Rapid innovation is inevitable, as no company can afford to stand still.
- Intellectual property rights play a ever greater role in competitive strategy.
- Very strong economies of scale are evident, with most costs being "first copy cost" with incremental costs of additional copies being far smaller than the average cost.
- Complimentary vendors need to be nurtured, as delivering end business value depends on complex interactions of systems and services from many suppliers. The "tight binding" through interfaces is a defining characteristic of the sector.
- Economy of networks results in larger players enjoying both lower unit costs, and stronger customer pull as large networks offer greater value than small networks.
- Economies of scale play a pivotal role, with a risk that monopolies will emerge, and that the resulting market power will potentially be abused if incumbents stifle new innovation that could threaten their established positions.

There are established cases in the IT industry (e.g. Microsoft versus Netscape) where regulators intervened after it became clear that a company that has held a dominant market position for several years or more, could be abusing its position to stifle innovation.

It can be argued however that the harmful effects do not yet apply even to the large Cloud computing providers, firstly as the market is still relatively new and evolving rapidly, secondly as to a significant extent growth is being achieved by displacing business from the established market of packaged software providers products being deployed by large systems integrators.

However, for the marketplace to be sustainable, it is essential to recognise relevant market characteristics including:

- Cloud computing services are far from homogenous. At the SaaS and PaaS levels most services are unique; for example there is no other supplier who offers the specific combination of services within Google Apps. While the IaaS level is the closest to homogeneity, for example at the x86 "server as a service" level, even here there is considerable differentiation between vendors for example in areas such as storage and network configurations, resilience options etc.
- there are clear entry barriers; for example establishing the brand and reputation that is needed for a Cloud computing supplier to be trusted with customers' data.
- likewise there are exit barriers; there will be an overhead for a customer to transfer data from a Cloud computing provider either back in-house or to an alternative supplier.
- transaction costs are significant; for example the cost of assessing the fit of a Cloud computing vendor's services to business needs, validating the contract, establishing trust etc.
- scale economies apply to the delivery of Cloud computing services; indeed it is scale economies that have catalysed the opportunity to achieve a new lower price level for certain categories of ICT service.

While acknowledging the above limitations, we concluded that the advent of Cloud computing enhances ICT consumers' ability to compare service characteristics and prices 'on-line'. It thus provides a significant step towards a more competitive ICT services marketplace, especially when compared to the established model of appointing a systems integrator to undertake the "specify design build test run" applications development life-cycle. However, it is also necessary for government's to establish appropriate commercial policies for use of Cloud computing services; those we identified are set out in section 10.6.

10.5 Development of the marketplace for Cloud computing services

A report published by the CBI in September 2012 titled "Open Access -- Delivering quality and value in our public services" [45] identifies the scope for significant cost savings from opening up more public services to private sector provision. The CBI argues that government must lead the agenda, and that government must be "an effective market manager" to ensure that the best providers from all sectors have the opportunity to contribute.

The same principles can arguably be applied to the provision of the Cloud computing services needed by a large-scale organisation for handling sensitive information and for creating

sophisticated end-to-end business processes. This supports work done during the G Cloud program phase 2 that concluded that public sector organisations are likely to evolve towards use of “hybrid cloud”; ie a mix of public, private and community cloud services, that will be used together with existing enterprise ICT.

This assessment is supported by an examination of the current uses of Cloud computing services within the UK.’s Ministry of Justice (2012). Here usage of cloud services includes:

- public cloud services such as Huddle being used for collaboration, and Microsoft 365 CRM for an interventions database.
- private cloud services, such as the “managed technical environment”, a private cloud service provided by HP for provision of development and test services to underpin development of prison ICT.
- community cloud services, such as the planned use of HP’s desktop 360G Citrix-based thin client desktop platform which is capable of being shared between government departments, creating potential for example for a shared platform providing service to both the Department for Work and Pensions, and the Ministry of Justice.

10.6 Desired commercial outcomes

During Phase 2 of the G Cloud programme we endorsed proposals from the Commercial Strategy workstrand to recognise “commercial principles” that would underpin the establishment and operation of an open and successful market for Cloud computing services. We also considered what incentives would be necessary to get the transition to Cloud computing services underway:

The principles are set out in sections 10.6.1 and 10.6.2 below:

10.6.1 Creating an open market for each service category.

Creating open category markets requires some form of marketplace (electronic rather than physical), that is open to new suppliers, and where consumers can readily identify, compare and purchase the services they require. This will be underpinned by:

- "making change simple and easy to achieve"; through putting in place the prerequisites for a marketplace where purchasers can switch easily between providers, ie:
    - a simple and open process to achieve commercial and technical transfer in and out of services, with
    - contracts of limited durations, while
    - ensuring there is choice of suppliers, and
- transparent and comparable pricing; requiring standard commoditised service definitions and commercial terms, together with published pricing thus enabling genuine comparability of services, and
- a standardised purchasing model; a standard approach to minimise transaction costs that is efficient from the perspective of both supplier and consumer.

10.6.2 Successfully running the marketplace once established

We also endorsed the proposal (from the commercial strategy team) that a market regulator is established to ensure the internal marketplace for Cloud computing services remains competitive and vibrant. We provisionally named this the 'G Cloud authority':- its role would include accrediting services and ensuring they meet technical, commercial and information assurance standards. It was also recommended that:

- savings are maximised through sharing customer owned intellectual property across suppliers.
- suppliers and end-user organisations are expected to comply with a mandatory governance and operating model.

With hindsight, these proposals appear too interventionist given that the marketplace is still undergoing rapid change and innovation. The approach proposed above creates the risk of inhibiting competition, firstly due to the cost overhead involved in accreditation, secondly as the time the process will take will result in delay. The consequences could be that ICT users are restricted to buying a limited range of services that do not represent the best option in terms of either value for money or functional competitiveness.

10.7 Achieving transition

10.7.1 Overcoming inertia

ICT System Integrators' current business models are primarily based on making a margin on the selection, integration and configuration of a range of hardware and software products to meet a customer's unique requirements. Today's suppliers specialise in building solutions that address the unique needs of their customers, and this uniqueness has inhibited achieving scale economies, including development of expertise in the design and operation of very large industrialised data centres. Thus the transition to Cloud computing presents incumbent ICT suppliers with a threat from two dimensions; firstly the unit pricing levels in the Cloud computing marketplace are significantly lower than those currently prevailing, secondly incumbent suppliers may not possess the experience or the competencies needed to lead in the provision of Cloud computing services.

Simultaneously, there is "inertia" on the buy side too. The in-house ICT departments of large organisations will in general have a cadre of staff with expertise in the conventional "design build test run" approach to ICT projects. Cloud computing requires however a new approach from internal ICT functions; for example the Canadian government [88] have recognised that "the CIO, who is gradually becoming a broker of IT services with a business-first mentality that guarantees a service will be delivered via the best method possible. In the future, a service could delivered via IT internally or through an external cloud provider, depending on the needs of the business".

Potentially, some members of internal IT departments may find this type of change threatening, as use of Cloud computing services requires some different skills, and thus there is a risk that those who do not have the necessary knowledge or aptitude could face redeployment or even redundancy as result of the introduction of Cloud computing-based approaches.

If not proactively addressed, there is potential for staffs' concerns over the potentially threatening implications of moving to a Cloud computing based model to undermine the transition, creating a degree of an in inertia and resistance that inhibits progress.

To mitigate such risks, IT leaders may wish to consider adopting proven corporate change management approach, for example that outlined in "Corporate Turnaround" by Stuart Slatter

and David Lovett [96]. The model set out in this book emphasises that purely having the pressure for change is insufficient to bring around effective change in large organisations; in addition it is essential to have leadership and vision, capable people, actionable first steps that can engage everybody, and effective rewards for individuals for making the transition.

10.7.2 The need for three simultaneous transformations

In the context of the need for:

- industrialised, automated, e-enabled large scale ICT capability, and for
- suppliers and buyers who individually and jointly embrace the potential of the Cloud computing model,

the G Cloud commercial strategy team identified that three simultaneous transformations are needed:

- Technology: Transitioning to industrialised, automated, digitally enabled physical ICT delivery infrastructure.
- Commercial process: Creating an enterprise class marketplace for Cloud computing services.
- People, skills and operational processes: Achieving a change in culture and behavior amongst both the buy side and sell side of ICT.

Achieving a single transformation is challenging in its own right, with many organisations that attempt such exercises failing. We concluded that successfully achieving three simultaneous transformations is of course yet more challenging, particularly as these cross organisational boundaries. This again supports the finding from previous chapters that, from a practical perspective, a phased approach to adopting Cloud computing services is inevitable.

10.7.3 A practical approach to phased implementation

Taking the above into account, the way forward is likely to reflect the “innovate, leverage and scale/commoditise” cycle cited by Christiansen (S Curves) [46] and others, as summarised below.

- **Stage one – Innovate**
  - adopt public cloud services where there is good fit with business needs, likely to initially be for relatively straightforward activities, eg hosting citizen facing websites, or providing in-house collaboration services.

  - commissioning private cloud services where there are recurring needs where costs can be reduced by having a 'private' or configurable/reusable platform. Provision of development and test services is a good example, or thin client desktop services initially for internal use.

- **Stage two – Leverage**
  - publicise users experiences with cloud services across the organisation or community. For example sharing experience on the use of public cloud services may result in identification of additional "value-added" opportunities through organisations using the same cloud service across organisational boundaries, and pooling experience on how to use a service to solve particular business requirements. This process should encourage collaboration between organisations, including sharing expertise on the private cloud services that have been commissioned for internal use.

  - where it becomes clear that multiple organisations have the need for what has been put in place as a private cloud service, enable this to be shared between organisations, enhancing the service to become a "community cloud service".

  - where new "complex line of business applications" are being created, provide an incentive for organisations to do so using "service orientated architecture models", and to make the component services available as "platform as a service" services (APIs) that can be reused by others.

- **Stage three - Commoditise and scale**
  - encourage development of cloud service broker and integrator capability with incentives to identify lower cost approaches for replacing established "legacy applications". This could involve encouraging an entrepreneurial approach, where the service broker is invited to review existing information-based services, and where there is an economic (or other) strong case for doing so, to propose that the service is

provided using an alternative “Cloud computing services” based approach. Such approaches would likely involve a hybrid blend of public, private and community cloud services, selected and managed in a way where together, the combined service package will meet the customer’s requirements for functionality, performance, resilience, security, transparency and transferability etc

- once the initial benefits of “remediation of legacy” have been achieved, encourage commodity provision of the “services orientated architecture” services that have come to dominate. This would involve creating a Platform as a Service capability with a series of reusable APIs to provide access to commonly used services. Implementation would involve a group representing the customer organisation taking control of the overall specification of major SoA services, and inviting others to offer exactly equivalent services and compete on price to win existing business. Again there would be a role for the cloud services broker in selecting the “best market option” on behalf of user organisations, integrating cloud and enterprise services, and managing the transition, delivering repeated cloud price reductions to customers. Competing in this marketplace would require the cloud services to deliver progressive cost savings.

10.7.4 Relevance of Service Orientated Architecture (SOA)

In their paper Service-Oriented Cloud Computing Architecture [80], Wei-Tek Tsai*, Xin Sun, and Janaka Balasooriya set out the relationship between SOA and cloud computing, specifically, “SOA is an architectural pattern that guides business solutions to create, organize and reuse its computing components, while Cloud computing is a set of enabling technology that services a bigger, more flexible platform for enterprise to build their SOA solutions. In other words, SOA and cloud computing will co- exist, complement, and support each other.“

This is consistent with the conclusion we reached during phase 2 of the G cloud programme;- specifically we recommended that an SOA-based approach be adopted to ensure that services are specified, selected, advertised and configured to ensure re-usability. Achieving a dynamic marketplace is more likely if the SOA framework is owned and controlled by the customer community; otherwise there is a danger that incumbent cloud service providers will seek to

inhibit competition by restricting the ability of new entrants to provide fungible alternatives to existing services.

10.8 Chapter conclusion -- The marketplace for Cloud computing services is not perfectly competitive, with providers deliberately and extensively differentiating services

From the buyer's perspective, there would ideally be a "perfectly competitive market" for Cloud computing services. However, while Cloud computing represents a step towards this ideal, there are significant shortfalls including lack of consistency of services, significant entry and exit barriers (costs), and high transaction costs for corporate customers.

The commercial barriers are lower where organisations' requirements are relatively homogenous, and can therefore be satisfied by a number of Cloud computing services on an "as is" basis. For example hosting websites, commoditised applications such as e-mail and basic word processing, and development and test services are well suited as starting points.

Developing a more competitive marketplace will require time, and could potentially be stimulated by the specification of standards that will apply across a large community group such as government. This will be enhanced if such standards can be aligned with those being specified, for example, by the EU or US governments.

From the commercial perspective we recommended that a systematic approach should be adopted that ensures that changes are simple and easy to achieve, that pricing is transparent and comparable, that purchasing is via a standardised model, that provides confidence that suppliers will meet minimum technical, commercial and information assurance standards and that there is a common governance framework that provides confidence that service specifications and standards will be maintained on an ongoing basis. The policies we proposed to address these goals are included in the G Cloud founding principles, which are set out in section 11.4.

In common with the technical, service management and information assurance areas, from the commercial perspective a phased approach will again be needed, starting by building experience and confidence in use of relatively simple services in lower risk areas of business, and then building experience over time.

11.0 G Cloud Phase 2 proposition

11.1 Introduction

Based on the findings that have been considered in previous chapters, we considered the options for the UK government Cloud computing strategy. These were documented in "the founding principles" [54], and in the 'G Cloud business case' [47] that compared the alternatives and recommended the way forwards. This was produced in spring 2010 (a few months before the general election). This chapter considers the assessment and recommendations made in the founding principles and in the business case.

A prevailing theme of the research summarised in previous chapters is that Cloud computing has the potential to bring substantial benefits through:

- economies of scale, as services can be shared between multiple user organisations.
- enabling organisations to have access to new services, including many that would otherwise be deemed unaffordable if the purchasing organisation had to cover the upfront costs of creating the new service.
- allowing ICT functions to respond much faster to new requests from business users, thus helping organisations enhance their competitiveness and thus growth rates.

The combined effect of the above benefits has the potential to bring substantial advantages in many organisations, and if there were no barriers or downsides, transitioning to this new model would become a "competitive necessity".

Previous chapters have also identified multiple downsides and the main barriers in transitioning to the public cloud, concluding that a hybrid mix of public, community and private cloud services will be needed, and that transition will be need to be phased over several years,

11.2 Barriers to take up

There are many issues that need to be addressed for successful and secure use of Cloud computing services. In some cases overcoming these issues requires that organisations assemble new skills, and in all cases there is a cost.

Examples of the issues that need to be addressed include:

- understanding the acquisition costs for Cloud computing services, including the overheads of assessing cloud providers' standard commercial terms (which are often on a take it or leave it basis), and the financial risk associated with some of the (potentially hard to quantify) risks of using a shared service platform that may be based in a different legal jurisdiction.
- establishing trust in the cloud services provider.
- overcoming the complexity of day-to-day management of ICT services, for example where the root cause of the service issue could reside with one of a number of service providers, all of whom may initially disclaim responsibility.
- the impact on end users of having potentially to cope with many different "user interface" designs provided by multiple organisations.
- the implications of corporate data becoming fragmented across multiple cloud providers.

11.3 Using Cloud computing services to implement business processes

11.3.1 "Stand-alone" business processes

As set out in earlier sections, barriers to use are generally lower where there is potential for genuine "stand-alone" use of Cloud computing services. This applies most readily in cases where there are relatively standardised, generic and recurring requirements for example:

- e-mail for example at the NHS which has introduced a multi-tenanted private cloud e-mail service (NHSmail), that enables many hundreds of NHS trusts to each configure and manage their own e-mail services, all of which are provided from a single secure platform.
- collaboration services, an example is Huddle [5] which is used by over 100,000 businesses globally including 60% of UK government departments for sharing documents and files, as well as enabling searches for people working in similar fields
- web hosting, for example the announcement [36] in September 2012 by the UK Government Digital Service (GDS) that it had signed a contract worth £600,000 with secure cloud provider Skyscape to host the new pan government single domain website gov.uk.

11.3.2 "Line of business" processes

However, while these "stand-alone" types of usage represent important first steps that will help build familiarity and confidence in the use of cloud services, due to the large number of complex processes, and the many tens of millions of citizens to be serviced, it remains the case that the majority of investment/cost in enterprise/government ICT is on "line of business processes"; i.e. the automation of core business activities. These processes are typically complex, and it is common to find that organisations have sought to improve customer service standards and reduce costs by putting in place automated "end-to-end" business processes that use a variety of data sources in multi-stage processes to complete a transaction or information request.

11.3.3 Recurring services involved in creating business processes

Delivering rich, high value-added processes such as those above requires access to and integration of a wide range of "component services", for example:

- employee authentication.
- select highest priority work item.
- validate customer identity.
- identify customer needs and select appropriate transaction.
- gather data.
- provide information.
- initiate transaction.
- pay and/or collect money.
- initiate requests on suppliers/agents/third parties, and log for automatic follow up.
- issue confirmation documents to customer.
- update records.
- create audit file.
- update management information file to enable future analysis of workload patterns and customer demand etc

One of the intentions of the G Cloud programme was to establish a services orientated architecture governance framework, that will allow sharing of services such as the above across government departments, thus reducing the number of services needed and the costs of maintenance. A study published by Assy [3] in 2013 identified considerable scope for rationalizing business processes within a telecoms firm, and found that the number of unique

services needed can be reduced by over 60%; this is consistent with the G Cloud team's projections.

11.4 G Cloud founding principles

We developed an approach to enable flexible use of Cloud computing services to support complex business processes. This was set out in the document titled "G Cloud Founding Principles" that was subsequently published on the Cabinet office website [54]. The core elements of the "founding principles" are summarised below; they include a recommendation to form a G Cloud Authority to arbitrate (or broker) between government departments and cloud services providers; the intention was to "do once" the complex discovery and assurance work on behalf of the whole public sector, rather than have this done many times, and at duplicated expense, by individual end-user organisations.

11.4.1 The G-Cloud Authority

One of the key roles proposed for the G Cloud authority was to provide the enabling framework for the use of multiple cloud services to deliver specific government services, while simultaneously avoiding substantial overheads in validating and then managing each of the component services individually. It was recommended that the G Cloud Authority would manage the interface between government and cloud services providers, and promote (and where necessary mandate) the use of approved cloud services by public sector organisations.

Effectively the G Cloud Authority would aggregate demand from across public sector organisations, help consuming organisations source cloud services that meet agreed technical, commercial and security requirements, provide integration and management services and (probably over a period of around a decade) lead a progressive transition process from the established ICT delivery model to yield the full commercial and agility benefits of cloud services model.

In doing we identified that the following services should be provided;- these are grouped below into the categories identified by Gartner [50] ie aggregation, integration and customisation [10]:

11.4.2 Aggregation services

The 'aggregation services' proposed for the G Cloud Authority comprise:

- facilitate agreement on commercial, technical, service management and information assurance standards across public sector organisations.
- forecast future demand from public sector organisations for ICT-based services.
- set minimum security standards for services, suitable for citizen facing websites, services relying on use of citizens' personal data, large aggregated data sets etc.
- set the expectation, and create the cultural environment, where public sector bodies do not commission new services for needs that can be readily met by existing services.
- commission the sourcing of a range of public, private and community cloud services (together comprising a hybrid cloud). NB: all cloud services would be "multi-tenanted", and would be capable of being "instantiated" for each purchasing organisation in the context of that organisation's data and specific configuration requirements, without these organisation specific aspects being visible to or accessible by other organisations using the service (unless this had been specifically permissioned by both parties as described below in the section on integration services).
- provide a online portal, (now launched as the CloudStore), to enable public sector organisations to access Cloud computing services regulated by the G Cloud authority. The intention is that with services on the CloudStore already having been procured onto a framework, they can be "called down" as needed, with detailed information on the service being available online, including non-functional characteristics, pricing and "satisfaction ratings" from current users of the service.
- oversee the certification of services (with the work generally carried out by the first organisation to use the service), with certification providing confidence to all users that compliance requirements have been met.
- commission a range of services suitable for hosting legacy applications, on the basis that these will continue to be needed for a lengthy transition period during which there will be an expectation of migration to the cloud model, i.e. in the period before the service is recreated in full compliance with the G Cloud (SoA) model and standards.

NB: In all cases the G Cloud Authority would be a "single customer" purchasing services on behalf of the public sector, and would pass on the benefits of the economies gained from scale and standardisation to the public sector bodies that are purchasing services.

11.4.3 Integration services

The 'Integration services' proposed for the G Cloud Authority comprise:

- provide the ability for cloud providers to deliver services to public sector organisations at their physical locations using a secure networking capability (the public sector network).
- provide a services interchange, to enable a business process (in real time) to call on multiple services sourced from across the G Cloud portfolio.
- provide a data conversion service that can be used to remap records and files for exchange between different G Cloud services according to defined configurations and mapping.
- provide a permissioning mechanism that will allow sharing of data sets (where appropriate) between trusted organisations.
- provide a standard set of infrastructure components that can be used in the creation of new business processes, to include for example employee and citizen authentication, make and collect payment, produce secure document etc.
- services to enable public sector "business communities" (e.g. organisations that have a shared customer group or other shared interest, such as health, welfare, justice, etc) to create integrated business processes that would span organisational boundaries. For example in the justice sector, to enable automated casework across the Police, Crown Prosecution Service, Her Majesty's Courts and Tribunals Service and the National Offender Management Service.

11.4.4 Customisation services

The 'customisation services' proposed for the G Cloud Authority comprised:

- an integration platform to enable new services to be created from existing services (NB: this would also allow configuration of the underlying cloud services using facilities inherent in the standard API, as well as the creation of a "overlay" that could provide a dedicated user interface optimized to the needs of the consuming organisation).
- a cross cloud business process management service(s), that would enable creation of a specific community business process, leveraging the integration services described above.

11.5 G Cloud Business Case

11.5.1 Introduction

Having designed the overall approach, there was extensive consideration by the G Cloud programme team on how to mobilise the initiative.

A detailed business case was produced in April 2010 [47] that set out the options for proceeding, and recommended the way forward.

11.5.2 Business case methodology

The business case was developed by a team of 10 individuals (including civil servants, ICT supplier representatives and economic/financial specialists) over a four-month period. It built on previous work undertaken between December 2008 and July 2009.

The team established a government ICT cost baseline that was used as the basis for subsequent economic and financial analysis; this was extended out to 2020 on the assumption that current government approaches and industry efficiency savings trends were sustained. The business case recognised that new policy driven initiatives may need to proceed at pace using conventional approaches, and thus did not assume any savings on such new initiatives.

A “long list” of options was identified through a series of workshops to help evaluate choices around the programme’s:

- scope
- service solution
- delivery approach
- implementation approach
- funding model

This process resulted in the creation of 1080 option combinations, derived from there being three scope options, five service solution options, five service delivery options, four implementation options and three funding options

Of these possible 1080 permutations, the most advantageous 11 were selected onto the “long list“, of which four were subsequently shortlisted. These four were evaluated together with two

other options, “do nothing” (i.e. retain current approach) and “maximise short-term savings” (i.e. minimise expenditure and maximise benefits in the period 2011 to 2014)

The six options that were compared are:

1. Do minimum (base case).
2. Data centre consolidation (without the introduction of Cloud computing services).
3. Establish a private cloud, and transition existing services to the private cloud over a ten-year period, as current contracts expire.
4. Establish a private cloud, and proactively transition existing services to the private cloud over an accelerated timeframe.
5. Establish a hybrid cloud (build a private cloud and use public cloud services),, and transition services in over a ten-year period, as current contracts expire.
6. Establish a hybrid cloud (build a private cloud and use public cloud services), and proactively transition in existing services over an accelerated timeframe.

11.5.3 Potential cost savings

The starting point for assessing potential cost savings was the estimated £16.9 billion of annual spend on ICT across the public sector in 2009/10, Of this, the business case assessed that the transition to Cloud computing could potentially realise annual savings of between £1.9 billion and £3.8 billion by 2020 (between 15% and 25%). These savings were estimated on the assumptions of lower unit pricing of services (resulting from aggregation of demand), including the impact of sharing services between departments. The business case also identified the scope for further non financially quantified benefits in the areas of:

- being able to deliver new ICT solutions faster and more flexibly.
- achieving further substantial cost reductions through the development of enhanced online services that can more quickly meet the demands of the UK population.
- achieving cost reductions by promoting efficient reuse of assets, as well as by promoting common approaches and automated services.

With the constraints of the economic climate that has prevailed since 2008, it was clear that upfront investment would need to be minimised, and short-term cost reductions maximised. This in turn led to recommendations to:

- prioritise the development of the application store for government (now launched as CloudStore).

- prioritise data centre consolidation.
- sweat existing assets unless replacement results in significant cost benefits.
- postpone applications consolidation and migration to 2014, which is when it was proposed that the full transition to the G Cloud model would start, delivering substantial additional benefits.

In the above context funding was sought to establish a government cloud services brokerage (the G Cloud Authority) that would initially focus on:

I. Implementing a governance and commercial model to enable the mandation and control of ICT procurement.
II. Supporting public sector organisations that could demonstrate an immediate business case for pioneering the use of Cloud computing services (usually publicly available services), designating these public sector organisations as "foundation delivery partners", and putting in place appropriate certification so that the selected services could subsequently be readily reused by other organisations.
III. Initiating procurement of a number of "infrastructure as a service" offerings that could be used across government.
IV. Identifying existing reusable assets and services that have already been procured by public sector organisations, and publishing these within the CloudStore.
V. Developing a plan to consolidate data centres that are in use by government.

The business case identified the need to achieve critical mass and traction within 18 to 24 months, through demonstrating that significant benefits can be obtained by the early adopters.

Threats and mitigations were also assessed, and included inability to secure funding, inability to establish the G Cloud Authority, inability to generate buy in and commitment of stakeholders, inability to generate sufficient savings and inability to successfully address security and information assurance concerns.

11.5.4 Strategic case

The business case sets out the context of the "user driven, organic growth" of the government ICT estate that has taken place over several decades, and how this has led to proliferation at multiple levels, with there being an estimated 130 data centres and 8000 server rooms in central government, together with around 90,000 servers running at utilisation levels that on average

are less than 10%. The business case explains how the previous approach to ICT made it difficult to:

- achieve cross government economies of scale.
- deliver quality systems that are flexible and responsive to demand.
- quickly take advantage of new technologies.
- provide consistent security controls.
- protect against major natural or human initiated incidents.
- meet environmental and sustainability targets.
- procure in a way that results in a dynamic and responsive supplier marketplace.

The strategic case is founded on technological, commercial and business processes advances in the ICT industry, with demonstrable efficiencies in ICT provision having been achieved by large scale cloud operators including Amazon, Bechtel, HP, Microsoft, and Google. For example Bechtel has cited a 60% reduction [1] in the costs of internal ICT through transition to a private cloud model.

Five main categories of benefits were identified:

- business enabling benefits, including flexible delivery of integrated services, providing organisations with a wider choice of services, and driving business efficiencies through sharing data across business communities such as welfare, justice, health etc.
- cost reduction, through increased utilisation of assets (thus requiring fewer assets), reuse of existing business solutions and reductions in the number of data centres.
- providing enhanced business flexibility (agility), for example through rapid scaling up and down of capacity needed for citizen facing websites (e.g. on announcement of a risk such as a flu epidemic), and for ICT's internal purposes (e.g. sourcing development and test, volume test and disaster recovery capacity etc).
- commercial agility, including shortened procurement timescales resulting from pre-certification of applications/services, and reduced unit pricing through the preference to purchase commoditised services that can be readily benchmarked.
- improved governance and assurance, including higher standards of information assurance (with common assets being assured once, rather than multiple assurances of similar assets), consistent supplier governance by the G Cloud authority on behalf of many public sector organisations, and with central oversight bringing improved compliance with licensing and related conditions.

The strategic case also identified that while some upfront investment would be needed to initiate the delivery phase of the G Cloud programme, the net effect would, relatively quickly, be to reduce capital investment requirements as Cloud computing is purchased on an "as a service" basis.

Strategic risks were considered, with it being acknowledged that cloud services are more suitable for services requiring lower levels of protection of integrity, availability and confidentiality.

The main risks were identified as being:

- lack of funding for initiating the programme.
- failure to secure senior stakeholder buy in may inhibit service take-up.
- the G Cloud Authority (internal cloud services broker) does not receive the empowerment and authority needed to drive implementation with public sector organisations.
- stakeholder management is not sufficiently effective to bring together currently duplicative procurements and other processes.
- the programme does not demonstrate sufficient cashable savings to secure ongoing funding.
- the pressure for cost reduction is such that the pricing and other commercial terms imposed on suppliers is insufficient to justify the necessary supplier investment in achieving transition.
- ICT suppliers undermine the programme by building momentum for proprietary "cloud" services that inhibit achievement of programme objectives.

Mitigations for all the above risks were identified, and are set out in the "G Cloud: Strategic Outline Business Case [47]).

11.6 Chapter conclusion – the G Cloud business case conservatively projected ICT cost reductions in the region of 15% to 25%

The overall conclusion from the business case (that was produced in cooperation with the supplier community) was that, once fully implemented, the Cloud computing model brings the potential to reduce public sector ICT costs by between 15% and 25%. Additionally services could be re-engineered to address the "digital by default" public service delivery agenda, and the ability to implement new government policies would be accelerated.

It was recognised that the transition would need to be phased over multiple years, and that it would be at least 10 years before implementation would be complete. The recommended starting point included establishing CloudStore (the application store for government), consolidating data centres, building use of commodity services, and establishing the G Cloud authority.

Potentially the cost savings set out in the business case were conservatively biased, given that the projected savings were based on input (with “buy-in”) from incumbent suppliers who had an incentive to downplay potential savings, and thus slow the decline from current revenue levels.

Part 3: Delivery of the UK government Cloud computing strategy in the period 2010 to 2013; successes, challenges and pitfalls.

This section analyses progress with the UK government Cloud computing strategy in the three years following completion of the strategy work in spring 2010. It considers the impact of a change of government, the progress that has been made, the challenges and key risks.

Previous chapters have concluded that Cloud computing has potential to bring substantial benefits to large-scale enterprises through wider choice, lower unit costs, plus reduced acquisition costs meaning that some services can be justified where they would previously have been deemed unaffordable.

However, there are also significant risks and costs for organisations in moving to widespread deployment of Cloud computing services, and as of mid 2013 many organisations are choosing not to use public Cloud computing services for any activity that involves (any level of) proprietary information.

Viewed 'top down' the key barrier is that most organisations lack the confidence to use cloud services for core business processes. There are justified concerns over security and compliance, including unintentional breach of legislation. In general organisations do not perceive that they have the capability and in-depth knowledge to overcome these and other key issues such as ensuring service continuity.

The starting point for using Cloud computing services in most public sector organisations is therefore for relatively simple non business critical activities services where risks are lower and more readily manageable; for example collaboration with other organisations. This may be supplemented by a "private (in-house) IaaS cloud" that provides a shared infrastructure platform, typically used initially for services such as development and test. Such "use cases" however only account for a relatively small proportion of ICT spend.

Potentially much larger benefits could be obtained if cloud services can be deployed to automate core high-volume customer facing business processes. Doing so however will typically require the use of a mix of in-house services (e.g. authentication services, access to data), and the use

of a range of external services integrated with case management, with business rules applied to determine the next step in the transaction. Using combinations of Cloud computing services in this manner is challenging because (as of mid 2013) there are not recognised industry standards for describing Cloud computing services or for achieving cloud interoperability. As a result organisations need to make a substantial investment in assessing Cloud computing services; pragmatically it is often more straightforward to continue with established methods.

A more practical alternative is to procure or create a dedicated range of private cloud services, for which the specifications and interoperability models can be controlled by the buying organisation. The services thus purchased can then be deployed in multiple contexts within the organisation, bringing benefits of lower prices through the consolidation of demand, and enhanced ability to share information. Public Cloud computing services can then be used in addition where they meet the business requirements (including security requirements), with controlled interaction with the private cloud services.

The above is in essence is what the G Cloud proposal set out in 2010.

The table overleaf provides a summary of the findings of earlier chapters on the potential benefits of using Cloud computing services, and of the issues that need to be overcome to do so successfully. The table also records an assessment of the theoretical ability of the 2010 proposal for "G Cloud as a brand" managed by the "G Cloud Authority, with the "green" ratings depicting the theoretical ability of the G Cloud Authority, with investment, to address the issues that had been identified.

The table is referenced in subsequent sections to provide a consistent basis for assessment of the reasons the various cloud deployment iniiativesc that have been attempted by the author have, or have not been, successful.

This table (with updated ratings) is repeated later in this thesis for the following assessments:

- Section 13.4: Assessment of G Cloud strategy as implemented.
- Section 14.4: Assessment of fit of public cloud services for "stand-alone" deployments that do not involve sensitive data.
- Section 14.4.1: Assessment of "moderate complexity" deployment.
- Section 14.4.2: Assessment of "high complexity/sensitivity" service.

- Section 14.5 Assessment of G Cloud fit against Ministry of Justice wide ICT procurement.
- Section 14.6: Assessment of pan government hybrid claimed proposal.

Section 14.7 then provides a comparison of the assessments, identifying the ranking of usage scenarios (best fit to worst fit), and the prioritization of categories of issue, and specific issues that need to be addressed.

Potential benefits of using Cloud computing services	**Issues to be overcome**
Cost reductions	The transition to Cloud computing services is inhibited by high costs and/or lack of skills needed skills for selecting, designing/securing, migrating data to, and managing Cloud computing services, and/or by legal/contractual constraints.
Accelerated innovation	Relationship imbalance; suppliers may be too big (or small) to take any individual customers needs/concerns into account
Meet consumers expectations in the mobile Internet era	Legal concerns over ability to assure compliance with rules on privacy, data residency etc
Increased choice and affordability of services for specialist needs	Lack of transparency of service design, security and management procedures
Flexibility to switch and scale use of services	Difficult to provide assurance that services meet their full specification
Dynamic supply marketplace to drive ongoing service improvement and cost reduction	Imperfect supply marketplace inhibits substitutability and thus price competition
Reduces risk by using well proven technology and suppliers	Information security risk – Inability to assure confidentiality, integrity and availability of services
	Inability to control future service characteristics
	Corporate governance frameworks unable to drive shift to Cloud computing, or ensure successful use of services and realisation of benefits
	Internal ICT organisations lack both the skills/culture for successful use of Cloud computing services, and the ability to build these for the future
	Overheads involved in selecting services proves prohibitive
	Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services
	The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive
	Some combination of the above undermines trust in business services that include a Cloud computing element

Table 2: G Cloud Authority: potential for delivering benefits and addressing obstacles to Cloud computing deployment
Code: Green -proposal addresses issue,
Amber proposal partially addresses issue,
Amber/red proposal partially addresses issue but only in limited contexts,
Red proposal does not address issue.

12.0 Obstacles encountered in implementing the G Cloud strategy

12.1 Context: Incoming government's policy objectives

Following the development of the G Cloud strategy and business case in March 2010, the imminent general election and possible change of government resulted in a pause and a period of internal review.

The May 2010 election resulted in a change of government. Incoming ministers placed greater emphasis on ICT's contribution to the UK growth policy and public sector cost reduction agenda.

The factors considered significant at the time were:

- The previous IT supply arrangements were seen as having excessively concentrated business with a small number of very large suppliers, who have been publicly referred to as "an oligopoly" [81]. The use of proprietary standards was considered to be a prime factor to the "vendor lock in" that had occurred, and the incoming government sought to mitigate this by emphasizing the desirability of use of open standards and open source code where possible.

- Austerity, which has had two major impacts:
    - Firstly, there was ever growing pressure on all parts of government to reduce costs. Specifically there was discussion about "curtailing gold plating", and moving from the previous government's philosophy that "public services (including the underpinning ICT) should be as good as the best in the private sector" to "good enough services delivered at the best possible prices".
    - Secondly, no funding was available for new initiatives. While the G Cloud business case promised substantial savings, it also required upfront investment likely to be in excess of £100m.

- Small and medium-sized enterprises (SMEs) were seen as critical to the UK growth agenda, and there was to be encouragement of SME friendly government procurement policies.

- There was a challenge on whether the business case for G Cloud, that promised savings in the region of 15% to 25% of ICT costs over a ten-year period was sufficiently ambitious. Specifically several commentators noted that some of the major cloud providers were citing that they had helped their customers achieve savings of up to 90%.

- A new policy ("digital by default") was announced to accelerate the shift in public service delivery to digital business models and approaches. It was not immediately clear whether the proposed G Cloud approach was sufficiently aligned with the "digital by default" policy. (It was recognised that it would put in place enablers).

In summary there was concern that the G Cloud team's recommendations would see government IT business continuing to go to very large suppliers, either incumbent system integrators or the emerging consumer focused cloud providers. Concerns were expressed on whether the G Cloud proposals would address inefficiencies in provision of government data centres, whether there would be sufficient opportunities for small and medium-sized enterprises (SMEs), whether there would be the desired shift towards use of open source and open standards, and also whether the outcome would make a sufficient contribution to the government's "digital by default" policy, rather than merely sustaining current models of public service delivery. There was also a challenge on whether the levels of cost reduction projected on the G Cloud business plan were the best that could be attained.

All of these issues were considered in detail, as discussed below.

12.2 Government ICT supplier landscape

By 2005, the majority of UK government ICT was supplied by a group of approximately 10 large suppliers. Such organisations had the scale and capabilities needed to take on large projects. However delivery had on occasions fallen short of expectations (although not necessarily more so than for delivery into private sector organisations), and the large suppliers incurred levels of overhead that meant that the solutions often seemed expensive.

Many of the G Cloud team of volunteers has been provided by the same large suppliers, and this prompted the concern on whether the "up to 25%" level of cost savings projected, and indeed the overall approach, really was the best that could be achieved.

Support for this challenge grew when comparisons were made with the scope for improvement in efficiency of ICT facilities and infrastructure provision. Concerns were reinforced by press reports that suggested that smaller companies had alleged that large suppliers had engaged in anti-competitive behaviour and collusion. The political goal of introducing an "SME friendly" government ICT procurement approach represented a significant shift from the policy of the previous government, which had even at one stage had an explicit objective of moving NHS ICT supply from a "cottage industry" [82] to larger suppliers. There was a perceived risk that the G Cloud programme's "Public Cloud First" recommendation would benefit the very largest cloud suppliers, as it is these organisations that achieve the greatest possible economies of scale and scope.

A further analysis of the maximum potential cost reduction attainable was conducted by the author, and is summarised below:

Cost category	2010 % cost allocation	2010 £m spend	Assumed potential reduction	Basis	Potential cost level attainable in 2020 £m
Desktop, office LAN and office productivity software	33%	1,333	50%	Comparison of cost of ownership with Google apps	666
Network	17%	667	25%	Internal projection	500
Data centre plant and infrastructure	25%	1,000	50%	Consolidate to 20 strategic facilities	500
Line of business applications	25%	1,000	50%	Use SoA based approach to achieve 60% shared components	500
Total	100%	4,000	46%		2,166

Table 3: Potential cost savings attainable if UK central government adopts cloud computing

This analysis, which indicates the potential for aggregate savings in excess of 45%, is approximately 80% - 200% greater than the level set out in the G Cloud business case. This later analysis thus supports the challenge of whether the G Cloud business case was being sufficiently aggressive in identifying potential savings. This outcome is also closer to the 60% savings reported by Bechtel [1] that has been mentioned previously. The case for targeting

larger savings is also supported by a paper produced by Federico Etro [95] which assesses that the savings available to public sector organisations through transitioning to cloud computing are typically in the range of 10% to 50%, and which cites specific examples that have achieved savings of 25%, 40%, 50% and 75%.

12.2.1 Data centre and infrastructure provisioning

A government-sponsored data centre study conducted in 2008 [83] had sought information from suppliers on the ICT infrastructure underpinning delivery to central government. It identified almost 200 separate physical facilities, together containing in the order of 100,000 servers that had an average utilisation estimated at 8%.

This was the first time that such an assessment had been made, and there was initially surprise and concern at the high number of facilities and low levels of utilisation identified.

Subsequent analysis by the author identified the underlying reasons for such diversity and utilisation levels. In summary this resulted from the outsourcing model that had been adopted. Specifically, ICT purchasing was typically done at the business unit (or government agency) level rather than for entire departments. Each agency tended to express its own requirements for data centre characteristics, and sometimes even for specific locations. An ongoing series of "urgent projects" together with preferences for "our" data centres to be sustained had resulted in proliferation of facilities, with minimal attention on the overall efficiency of data centre provision.

The low utilisation levels of the servers deployed in data centres resulted primarily from a "project by project" approach to procurement of computer systems hardware and operating software. Typically, as there were no "standard approaches"; each project would select the servers and software stack that were going to underpin its new business application. As well as the production hardware, there would be a need to purchase various other environments; these are set out in the table below together with their target long-term utilisation levels.

Environment	Capacity (relative to production environment)	Target utilisation level	Long term average utilisation on 24 x 7 x 5 year basis
Production	100%	70% during annual 'peak hour'	20% (assumes 60% average utilisation during the 'working day')
Disaster recovery	100%	0%	0%
Volume test	75%	10% while application development is underway	1%
Development environment	25%	20% (assumes 60% during the 'working day') while application development is underway	4%
Weighted average		25%	8%

Table 4: Low average system utilisation results from a project initiated approach to provisioning data centre based systems

From the table above is can be seen that overall, projects were typically purchasing three times system capacity needed to sustain the peak annual load for the production service. The average server utilisation of 8% that was being achieved in 2010 is thus around what was to be expected from the ICT deployment model in place at the time. This results from the model where individual projects purchase unique hardware, and thus need to provision multiple environments built to this specification even though the majority of them will be lightly used, with the extreme example being the disaster recovery environment for which the target utilisation is 0%!

By contrast, the "standard hardware platform" approach that underpins the Cloud computing model means that it is no longer necessary to put in place dedicated environments for development, test and disaster recovery; these environments can be provisioned on an "on

demand basis" for the periods when they are needed. The ability to migrate any workload to any data centre that supports a particular Cloud computing service enables very high levels of average utilisation; Google for example cite that their approach of adding you capacity "just-in-time" allows the achievement of a typically 98% utilisation level. This order of magnitude efficiency enhancement, together with additional savings that result from standardization, automated management systems, and scale of facilities including the ability to secure low-cost power supplies and cool locations underpins the cost advantage that the major cloud providers enjoy. (NB: The full cost advantages are not automatically passed on to customers.)

12.2.2 Involvement of small and medium-sized enterprises (SMEs)

A policy objective of the incoming coalition government in 2010 was to increase the share of new government ICT business won by SMEs, with the target being set at 25%. This represented a substantial challenge, in that at the time, the business won directly by SMEs was negligible. This resulted in part because SMEs typically do not supply at scale of necessary to meet government needs, or have the financial resources need to meet the "due diligence" tests on their ability to meet any claim for poor performance. To reinforce the political intention to move away from large contracts awarded to large suppliers, a new limit of £100 million was set on the maximum size of a contract award. While this is a substantial sum, it is approaching two orders of magnitude less than the largest comparable contract awards of the 2000s, which ranged up to £billions.

However, a core element of the G Cloud proposal was to move to a commodity purchasing model for ICT, where demand for standard services would be aggregated across government, and purchased from the supplier able to provide the best pricing. This was envisaged to provide opportunities for suppliers (through CloudStore sales) to generate business volumes potentially of several hundred million pounds, which would have enabled investment in efficient provision of private cloud facilities. Hence there was a further conflict between the G Cloud proposal and incoming government policy.

This resulted in a shift of emphasis in the G Cloud procurement to be much more open to SME participation. While this encourages a more dynamic marketplace, this does bring downsides, specifically fragmentation of the supply marketplace and greater need for greater due diligence by purchasing organisations. In certain cases, (specifically where cloud solutions are used in isolation in contexts where data is not especially sensitive) this does bring the benefit of reduced

overheads and greater choice of suppliers. For core business critical processes though (arguably the majority of cases), this creates barriers to use of G Cloud services, specifically that the fragmentation of supply means that suppliers may lack sufficient incentive to invest in producing appropriately secure services.

12.2.3 Open source and open standards

The incoming government placed increased emphasis on the use of open source code, and open standards throughout the ICT supply chain, citing the downsides of the previous approach, such as the high degree of "lock in" that had developed with products from suppliers such as Microsoft. For example in the National Offender Management Service alone, over a period of a decade or so in the order of 100 dependencies had arisen between national applications and desktop software. This brings benefits, for example enabling a probation officer using a national case management application to print a formatted letter using the word processing package. In parallel local business units had been encouraged to create their own applications building on the investment made in proprietary office productivity software;- 10 years later there were well over 1000 instances of such applications that make vendor specific calls on word processing, spreadsheet and database software. While from some perspectives these initiatives are to be applauded, they do have the side effect of creating "lock in" to a particular supplier of office productivity software, and thus transferring market power from the consuming organisation to the software supplier. Over time it becomes ever more impractical to migrate to a competitor's product;- meaning that there is limited choice other than to purchase upgrades and support from the incumbent. Significant investment will be required to move to open standards to break such supplier 'lock-ins'.

A key "lock-in related" concern expressed over the G Cloud strategy was that it would tend to place business with public cloud suppliers, who have developed their own proprietary standards for platforms such as Force.com and Google apps. Hence there was a perceived risk that the proposed approach would merely recreate lock in with a new set of suppliers, inhibiting UK government's ongoing ability to migrate to suppliers offering the best combination of product, service and price.

12.2.4 Alignment with "digital by default" strategy

Another issue that prompted debate was whether the G Cloud strategy supported the new government "digital by default" policy. This was defined as the intent to deliver public services over the internet that are "so straightforward and convenient" that all those who can use them will choose to do so. It was concluded that G Cloud could support the digital by default agenda, providing a cost-effective hosting environment that could pave the way for cross organisational sharing and reuse of both specific services, and commodity applications.

12.3 The G Cloud strategy was adapted to reflect the policy objectives of the incoming coalition government

The incoming government had the (entirely legitimate) objective of achieving a shift in the ICT supply-side marketplace. The G Cloud initiative, repositioned, has continued as it could align with some of these objectives in particular opening a route for SMEs to compete for government ICT business.

The major changes in emphasis can be summarised as follows:

From	To
Aggregation of demand, likely leading to the award of business to a relatively small number of highly efficient large-scale suppliers	Encouragement of a vibrant market of SMEs, who will be highly flexible and efficient.
A systematic programme to remediate legacy systems, and migrate core "line of business processes" to the G Cloud model to achieve cost reduction on the installed base.	Provision of a range of services that can be used to underpin new initiatives, in particular the "digital by default" agenda.

Table 5: Repositioning of G Cloud strategy following 2010 general election

This repositioning however moved G Cloud away from its original intent to consolidate ICT delivery on a combination of private cloud services and the most efficient (and thus the larger scale) Cloud computing providers. In particular, the large US based Internet firms such as Google, salesforce, Microsoft, Amazon etc introduced with their cloud services a new set of proprietary standards, and were thus not a good fit with the open source and open standards elements of the government ICT strategy.

At a time of focused cost reduction, it was decided not to allocate significant budget to the G Cloud initiative. While a small central team was established to support a procurement exercise to source cloud services, the budget was insufficient to mobilise the G Cloud Authority.

Nevertheless, it is a success that the G Cloud initiative has continued and is now achieving an increasing degree of take-up as described in following chapters.

13.0 UK Government Cloud Computing Strategy

13.1 Announcement

We announced the imminent publication of the modified government cloud strategy on at the Westminster eForum on September 13, 2011 [20] [28].

The (updated) G Cloud strategy (Cloud Computing) was then published in October 2011 [29], and this was followed by the launch of CloudStore [26] in Spring 2012 as an online catalogue for accessing both public and community cloud services that have undergone initial supplier and service accreditation.

The strategy embodies many of the core principles of the vision that was developed by the G Cloud programme team in 2009/10. It prioritises those aspects that can be progressed with lower expenditure and which maximise early benefits.

13.2 Scope

The strategy reflects many of the objectives proposed in 2010, and sets out the context of current issues with government ICT, including difficulty in:

- achieving large, cross government economies of scale.
- delivering ICT systems that are flexible and responsive to demand in order to support government policies and strategies.
- taking advantage of new technologies in order to deliver faster business benefits and reduce costs.
- meeting environmental and sustainability targets.
- procuring in a way that encourages a dynamic and responsive supplier marketplace and supports emerging suppliers.

13.2.1 Positioning

The strategy reasserts the principles of Cloud Computing and puts in place a “public Cloud First” policy. It sets the expectation that the G Cloud will be an assured collection of services that will grow over time, rather than being a single entity.

It sets out the intention for government to use multi tenanted services, that are shared and managed by several organisations. Also that “shared resources, infrastructure, software and information will be provided to a range of end-user devices, e.g. smart phones and laptops, as a utility on a pay by use basis, via a network connection -- in many cases the Internet”

The strategy sets out the benefits of being able to increase flexibility and agility in the way ICT is used, by buying services only when they are needed, i.e. “we should do it once, do it well, and then reuse, reuse, reuse”.

13.2.2 Benefits

The anticipated benefits comprise cost reduction and increased business flexibility. Targets for the take-up of cloud services are set.

A parallel enabler of the cloud strategy is intended to be the optimisation of the government data centre estate, acknowledging that this has traditionally been “hugely inefficient”. The strategy sets out the scope for delivering significant savings in cost, energy and accommodation costs.

13.2.3 Commercial process

It is recognised that changing the way government buys ICT is fundamental to achieving the desired benefits. Specifically it is acknowledged that this will involve “changing the culture of government ICT to adopt and adapt to the solutions the market provides and not creating unnecessary bespoke approaches”

A key element of the strategy is creating a more efficient market for ICT services, recognising that government departments can most readily adopt commodity ICT services where these are provided via mature markets that offer the customer genuine choice, and the ability to transfer to new providers where a better value proposition exists.

The government “marketplace” for cloud services was also announced with the working title government application store (now launched as CloudStore). The CloudStore provides “the window on an open, visible and commoditized and cost transparent marketplace”, that is the first port of call for any public sector ICT requirement, a “shop window where relevant services can be found”, encouraging innovation, competition and new suppliers, exploiting pan public sector purchasing, and providing the security and service management communities with access to detailed information on services.

13.2.4 People and governance implications

The strategy acknowledges the need both for behavioural change amongst the government ICT community, and for development of the supplier marketplace (which will take time). It sets out the intention (not yet implemented) to establish the G Cloud Authority to provide regulation, compliance management and some cloud brokerage capabilities.

13.2.5 Information assurance considerations

The strategy recognises that cloud services must all provide an acceptable level of security risk mitigation, and allow public sector organisations to demonstrate that they are meeting legal and statutory requirements.

13.3 Similarities between the published government Cloud computing strategy and the G Cloud Phase 2 work of 2009/10

This section summarises the areas where the strategy published in November 2011 reflects the proposals delivered by the G Cloud phase 2 programme team in Spring 2010. The common themes are:

a) The assertion of the basic principles of Cloud computing, and the rationale for switching from the established “custom business solution” approach that exists today.

b) The anticipated benefits including cost reduction, and increased flexibility.

c) The adoption of the US NIST (National Institute for Science and Technology) definition of Cloud computing, and the recognition of the four deployment models of public, private hybrid and community clouds.

d) The "vision" of using commodity-based multitenanted services, that are accessed via a network, purchased on a "pay per use" basis, and reused across government.

e) Recognition that "G Cloud" will not be a single entity, but rather an ongoing programme of work; this is aligned with the "G Cloud as a brand for trusted government Cloud computing" that was proposed in Phase 2.

f) The acknowledgement that a change in the way government buys and runs ICT will be needed to adopt G Cloud, and that this will bring changes and challenges in many areas, including procurement, transition, service operation, and meeting statutory and legal requirements etc.

g) The plan to establish a government application store (now launched as CloudStore) as an online portal, encouraging innovation, providing a marketplace/shop window, and consolidating purchasing power.

h) Recognition that a mature market for cloud services is needed, and that this will take some time to achieve.

i) Recognition that the development of the cloud services marketplace must provide attractive opportunities for suppliers if it is to happen.

j) The intention to establish a G Cloud Authority, and to give this organisation the power to mandate government departments to use cloud services.

k) The intention to put in place a management structure that (using a federated model) that can enlist government departments and other public sector bodies to build the momentum of G Cloud, with an inclusive approach, and within a standards context set by the G Cloud Authority. Additionally the "Cloud First" principle is set out; i.e. that where a suitable service already exists government departments should be expected to use it rather than create another.

l) The intention to maintain a strong connection between the deployment and adoption of G Cloud services, and the rationalisation of the current data centre estate.

m) The recognition that it will be essential to rationalise and migrate existing ICT services in order to implement the strategy; i.e. it will not be practical to achieve the G Cloud vision simply by using CloudStore to address new needs.

n) The intention to establish a G Cloud commissioning and adoption roadmap, underpinned by a strategic plan that will identify opportunities for government to introduce new cloud/community services.

o) That it will be necessary to establish a G Cloud programme to drive the transition, and that this will need to include a "foundation delivery partner programme" to support the public sector organisations that are acting as the commissioners (first users) of services that will be subsequently be made widely available for use by others.

p) That work will be needed in the service management arena to establish standard service metrics and a common model.

q) The intention to establish a pan-government cloud services Information Assurance regime, that will allow cloud services to be accredited once for use across the public sector. Consuming organisations will then use this assessment to decide whether the service, when used with the organisation's data, will meet the confidentiality, integrity and availability standards needed for that organisation/service. Such assessments will need to consider the sophistication and likelihood of threat by hostile parties, or by employees or legitimate users.

r) The need for a governance model that is linked to the overall government ICT strategy implementation approach.

s) The need to have clear benefit targets which are set out for the 12/13, 13/14 and 14/15 financial years as being savings of £15 million, £40 million and £120 million respectively for G Cloud, with in the corresponding (additional) benefits from data centre consolidation being £20 million, £60 million and £80 million respectively.

13.4 Implications of revised G Cloud strategy; Changes in emphasis from work done in 2009/10

There are some changes In the published strategy compared to the G Cloud vision developed in 2009/10.

As set out in section 12.3, compared to the intentions in the published documents produced by the G Cloud Phase 2 programme team in early 2010, the main differences in the strategy published in November 2011 is the creation of a SME friendly procurement framework, and the emphasis on deployments in circumstances where requirements are relatively straightforward and data is not highly sensitive. This approach does not however provide the capabilities to cost effectively create organisation specific "line of business processes" from commodity Cloud computing services; capabilities that are essential to address the majority of government's citizen facing ICT enabled public services.

Specifically:

a) Private cloud services are de-emphasised: There is a stronger emphasis on the "public Cloud First" policy intention in the November 2011 strategy document. As a result there is less emphasis than in the 2010 proposal of establishing a range of private and community cloud services that can be used where there is no suitable public cloud service (E.g. for migration of legacy services).

b) Community cloud: the strategy is silent on any intention to establish community clouds within government; the original view had been that additional new business benefits could be realised by enabling easier controlled sharing (where permitted) of information within business sectors such as health, welfare, justice, defence etc.

c) The application store, now launched as CloudStore, is primarily positioned as an on line catalogue. In the 2010 vision the CloudStore would also have enabled digital access to a range of services that would have supported deployment, integration, commissioning and management of selected Cloud computing services. This was an ambitious vision which is not generally supported by today's cloud services, and for which there is not a

recognised standards framework. The scope of the application store (CloudStore) has hence been reduced, at least initially. While the strategy published in 2011 acknowledges the need for support with design, development, transition and operation of services, (other than by appointing a suitable integrator) there is no suggestion that any automated services or support will be available through CloudStore. It is recognised though that organisations using cloud services will need tools to help with commissioning, decommissioning and switching services.

d) Service management model: while this is included in the strategy published in 2011, the scope has been reduced with greater focus on consistent management of services that can be used on a stand-alone basis. The strategy does not set out an approach for delivering SLA's for "business services" provided to end-users (specifically for business services that are composed from several cloud services). While the proposed service management model covers the design, development, transition and operation of services, and the collection and collation of service management information, it does not reflect the original vision of having a standard service management model that would enable guaranteed business service SLAs. This capability is still relevant given the intention to abstract the common business services used in complex line of business processes, e.g. payments, authentication and similar.

e) Information assurance model: although the principle of single technical accreditation of services on behalf the whole of government is sustained, the strategy is relatively silent on the roadmap that will be needed to enable consistency in the approach taken with the organisation specific information of each public sector body. Consistency of technical controls will be important to enable the sharing of (derived) services that are themselves based on G Cloud services.

f) Addressing the installed base (legacy): the 2010 strategy had set out a "roadmap" for progressively migrating existing government ICT-based services into G Cloud. The 2011 version set out the intention to "establish a commissioning and adoption roadmap", (NB: As of July 2013 work on this has not commenced).

g) Risks: the 2011 strategy identifies six main risks, four of which relate to internal issues. While it clearly signals that getting the many thousands of professionals working in government ICT aligned with new approach will be fundamental to success, (with the

exception of providing the G Cloud Authority with the right to mandate the approach), the strategy does not set out the timescales for initiating some of the work to address the more fundamental barriers to change.

h) Pace and planning: the published intention is that in the financial year 2014/15 around £200 million of Cloud computing business will be delivered through the new model. This is lower than set out in the 2010 business case.

i) For procurement of services, there is more emphasis on the use of frameworks, including "dynamic purchasing systems" that allow new suppliers to join existing frameworks where they meet requirements.

j) A major feature of the 2010 strategy was the approach for migrating existing government ICT services into the G Cloud framework, with the intention having been to drive this through on expiry of existing contracts. Specifically, commissioning of G Cloud services was to be done in anticipation of the government ICT contracts that were coming up for renewal in the next 12 to 24 months, so that the services provided through imminently expiring contracts could be readily replaced by the continuously expanding portfolio of G Cloud services. For complex line of business processes, this was to include sourcing "service-oriented architecture" components such as payments and citizen authentication; these would be built once and reused across departments. These aspirations are not reflected in the strategy published in 2011.

k) Linked to the above, the 2010 strategy set out the possibility of accelerating transition by "buying out" suppliers from existing contracts, as the range of G Cloud services increased, and the cost savings attainable by migrating existing services before the end of contract duration became ever more attractive. The strategy published in 2011 is silent on this point.

13.5 Risks

Fewer risks are identified than in the 2010 strategy, with the 2011 strategy identifying three main areas:

- Leadership, specifically the challenge of aligning the G Cloud and data centre consolidation initiatives with the other major elements of the government ICT strategy.

- Internal delivery capability, including availability of skills and knowledge needed to successfully deliver in the new environment, moving the prevailing "mindset" from "let's build another new solution" to "let's reuse what we've got", achieving effective end to end service management when using commodity multi tenanted cloud services that are shared between many organisations, and introducing an effective and efficient information assurance regime for public and private G Cloud services.

- Market/supplier response, with there being recognition that it's essential for the supplier marketplace to view the provision of G Cloud services as an attractive business proposition, given the need for upfront investment to make G Cloud services available on a "pay as you use" basis.

13.6 Comparison with other governments' Cloud computing strategies

This section summarises analysis of other governments cloud computing strategies conducted in early 2014.

13.6.1 Governments with a "cloud first" policy

As in the UK, both the United States [87] and New Zealand [89] governments have declared a "cloud first" policy that requires public organisations to adopt cloud computing unless there are clear reasons why conventional approaches will deliver a price or "better fit with requirements" advantage.

In the UK, this commitment has provided sufficient market stimulation for suppliers such as Skyscape [35] and FCOS (which is owned by the Foreign and Commonwealth Office) to invest in providing proprietary infrastructure as a service platforms that meet security and data residency requirements for the local public sector marketplace.

The UK is also seeing an increasing number of organisations offering cloud integration (or cloud brokerage) services, via lot four (services) of the G Cloud framework; this accounts for a substantial part of sales to date.

United States

Likewise in the United States [87], both Microsoft and Amazon Web services have established dedicated infrastructure as a service cloud platforms that achieve similar ends for US government organisations.

The US is adopting a different approach to cloud services brokerage, with certain public sector organisations stepping forward to take a lead role in the provision of cloud integration services. For example the Defence Information Services Agency [90] is undertaking this role for public sector organisations in the defence community, while the National Nuclear Security Administration is undertaking a similar role for the energy community.

The United States has developed policy to support the cross public sector use of Cloud computing services; specifically the National Institute for Science and Technology (NIST) has published a Cloud computing reference architecture [91], and a Cloud computing security reference architecture. There is a long established standard for implementing security requirements (FISMA), and there is a pan government accreditation approach (FedRAMP) [48] that enables accreditation work done by (or on behalf of) one government organisation to be shared and re-used as accreditation by others, thus avoiding non-value adding duplicative accreditation activity.

New Zealand

The New Zealand government [89] is "expecting" public sector bodies to adopt approved cloud computing services when addressing a new requirement, or when a contract is up for renewal.

13.6.2 Other governments with significant commitment to cloud computing

Australia [85] which announced a data centre consolidation program in around 2011, published in July 2013 a comprehensive approach to Cloud computing, which recognises the need for Cloud computing type approaches to provide the enablers needed for a "vibrant digital economy". Australia has published guides for public sector departments on Cloud computing

policy, an implementation guide, the approaches to privacy, meeting legal requirements, building business cases, addressing security considerations and governance of community clouds.

Canada [86], [88], where the "Shared Services Canada" initiative is seeking substantial savings through agencies consolidating data centres, infrastructure and applications. Canada have recognised that this has significant implications for the transformational role of the CIO, with a greater future focus on "the alignment of IT agility to business process improvement". Specifically they cite "the CIO, who is gradually becoming a broker of IT services with a business-first mentality that guarantees a service will be delivered via the best method possible. In the future, a service could delivered via IT internally or through an external cloud provider, depending on the needs of the business".

France [84], which is investing in a private infrastructure as a service platform, known as Andromeda, which will meet local data protection and other legislative requirements, and which is being supplied by Orange and Thales.

Singapore [87], which while encouraging public sector organisations to make use of commercially available public cloud services is also implementing a private infrastructure as a service cloud, and which is developing an approach to enable interoperability and sharing services across the whole of government.

Japan [87], South Korea [87] and Taiwan [87] who are all making significant investments in establishing community cloud services for public sector organisations, and in some cases also seeking export opportunities.

Germany [84], Ireland [84],, Spain [84],, Thailand, [87] Malaysia [87] , China [87](at local level) and Hong Kong [87] who have all signaled to public sector organisations that Cloud computing services should be considered and used where appropriate. Spain has also declared an intent to establish a private cloud for public sector organisations.

Denmark [84], which in response to cost reduction pressures has established a central ICT agency which is actively promoting cloud computing-based approaches.

13.6.3 Countries making slower progress

Some other countries are known to be looking at Cloud computing strategy, but where progress to date is believed to be relatively slow. These include:

- **India [87],**, limited progress seen to date, with no published strategy.
- **Indonesia [87],,,** where progress is inhibited by lack of a high-speed Internet capability.
- **Philippines [87],**,, where there is no central government ICT agency to coordinate policy.
- **Vietnam [87],,,** who are in discussion with IBM about a proprietary cloud solution.
- **Austria [84],,,** who have published a position paper.
- **Finland [84],**,, which is "moving towards having a strategy".

13.7 Chapter conclusion -- G Cloud announcement

The UK government's G Cloud strategy (Cloud Computing) was published in October 2011 [29]. The strategy embodies many of the core principles of the vision that was developed by the G Cloud programme team in 2009/10. It prioritised the introduction of the CloudStore but did not include a deterministic plan for establishing the G Cloud Authority or capabilities needed for Cloud computing to be used for business critical "line of business" ICT services, or those that utilise sensitive information, ie the services that comprise the majority of current activity and thus costs.

Embracing a "cloud first" philosophy, based on he comparison in section 13.6, the strategy places the UK at the forefront on the international stage in the intent to adopt Cloud computing services (ie via a "cloud first" strategy.

The UK strategy recognised that changing the way government buys ICT is fundamental to achieving the desired benefits, and this has been followed by tighter central controls to enforce the cloud first, open source and "digital by default" policies. There is still much work to do in achieving behavioural change amongst internal teams and development of the supplier marketplace.

The G Cloud Authority has not been established as a separate entity; rather there is the realisation that standards, in particular security related standards, need to be aligned across all

ICT infrastructure components; i.e. Cloud Computing services, hosting, network and end-user devices. Accordingly there has been active consideration of the formation of a single Public Sector Technical Services Authority to cover all areas of infrastructure standards

The major exclusions compared to the March 2010 proposal are:

- Standards for interoperability, burstability and transferability.
- Initiation of a business communities based approach for service commissioning and transition management.
- A framework to create composite 'line of business' processes from a series of cloud services.
- Development of a governance model and business plan for initiating a Services Orientated Architecture based approach to transitioning legacy systems to the cloud model.
- The 'integrated services manager' approach to ensuring that end to end help desk, and service management and assurance processes can be put in place for composite services.

The impact on the ability of the G Cloud initiative to deliver the benefits and address the obstacles that have been identified is summarised in Table 6 overleaf:

Potential benefits of using Cloud computing services	Issues to be overcome
Cost reductions	The transition to Cloud computing services is inhibited by high costs and/or lack of skills needed skills for selecting, designing/securing, migrating data to, and managing Cloud computing services, and/or by legal/contractual constraints.
Accelerated innovation	Relationship imbalance; suppliers may be too big (or small) to take any individual customers needs/concerns into account
Meet consumers expectations in the mobile Internet era	Legal concerns over ability to assure compliance with rules on privacy, data residency etc
Increased choice and affordability of services for specialist needs	Lack of transparency of service design, security and management procedures
Flexibility to switch and scale use of services	Difficult to provide assurance that services meet their full specification
Dynamic supply marketplace to drive ongoing service improvement and cost reduction	Imperfect supply marketplace inhibits substitutability and thus price competition
Reduces risk by using well proven technology and suppliers	Information security risk – Inability to assure confidentiality, integrity and availability of services
	Inability to control future service characteristics
	Corporate governance frameworks unable to drive shift to Cloud computing, or ensure successful use of services and realisation of benefits
	Internal ICT organisations lack both the skills/culture for successful use of Cloud computing services, and the ability to build these for the future
	Overheads involved in selecting services proves prohibitive
	Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services
	The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive
	Some combination of the above undermines trust in business services that include a Cloud computing element

Table 6: Implemented G Cloud strategy: potential for delivering benefits and addressing general obstacles to Cloud computing deployment
Code: Green -proposal addresses issue,
Amber/Green – proposal largely addresses issue
Amber proposal partially addresses issue,
Amber/red proposal partially addresses issue but only in limited contexts,
Red proposal does not address issue.

From the table above, it can be seen that while the initiative partially addresses some of the desired benefits and issues, the changes made restrict the ability of the G Cloud initiative to addressing only some of government's ICT needs, although possibilities will increase over time. The outturn of take-up and possible future mitigation steps is discussed in the next chapters.

From the analysis of other countries' approaches to government cloud computing, it is clear that the intent to embrace the benefits of the new model is widespread. As per the foundational work undertaken in the UK, many countries have recognised the potential benefits of establishing a

community cloud for the public sector, and of taking steps to establish standards and to build the capabilities needed to integrate and work with combinations of Cloud computing services.

14.0 Progress eighteen months after publishing the G Cloud strategy

14.1 Services available on G Cloud

Since the launch of the CloudStore in April 2012, there have been three procurement exercises (eg [31]) that (by end October 2013) have resulted in over 7000 services now being available from 800 suppliers. There have been almost 3,900 sales valued at over £63.5 million [30], and examples where savings of 50% to 90% have been achieved compared to conventional ICT costs. While the value of the average sale at £16,500 is relatively small in government ICT terms, the average cost of the alternative (displaced) option is assessed to be in the region of £40,000-£60,000. The Cabinet Office report that "56% of total sales by value and 61% by volume, from all reported G-Cloud sales to date, have been awarded to SMEs".

Around 20 of the 7,000 services have been accredited to meet the security and supply standards for citizen data, and this provides an embryonic opportunity to leverage this set of services in place of the private cloud capabilities described earlier.

14.2 Successful deployment examples

As was anticipated by the G Cloud team in 2010 (and in earlier chapters), it is more straightforward for public sector organisations to begin using cloud services for relatively "stand-alone" business needs, and as set out in chapter 14 this is what has been happening in practice. The main uses of cloud services by government organisations to date are for:

- Web hosting
- email and 'office' software
- collaboration services
- infrastructure as a service that can be used in an "non-integrated" fashion, including for storage, and for development and test services.

The outturn is in line with the survey conducted in April 2010 of local authority ICT leaders (reference section 6.5)

Some examples of deployments to date include:

- Windsor and Maidenhead Council are using a cloud based social networking tool to track and respond to residents' concerns
- Hillingdon and Warwickshire councils are using Google apps for e-mail and office software
- Ordnance Survey is using Amazon Web services to provide businesses with access to mapping services
- The Government Digital Service is using Skyscape's infrastructure cloud service to host the pan government gov.uk website
- The National Offender Management Service is using hosting services, collaboration and CRM services sourced through CloudStore.

A brief overview of each is provided below:

14.2.1 Windsor and Maidenhead Council

Windsor and Maidenhead Council serves approximately 140,000 citizens to the west of London. The council is using the salesforce chatter service (which is integrated with Facebook) to enable citizens to contact the council via social media (which themselves are typically cloud services). The Council reports this is enabling early detection of issues that are of concern to citizens, and better collaborative working both between council employees, and between council employees and citizens.

14.2.2 Warwickshire County Council

Warwickshire are planning to migrate from an "on premise" Lotus Notes deployment to Google apps. Deployment commenced with a pilot of around 20 users and was followed with a further pilot for all 250 users;- a greater number than originally planned due to the desire to extend the benefits of being able to collaborate on documents.

The main positive outcomes from the pilot are:

- Flexibility of access (including via smart phone and tablets) to e-mail and corporate documents was seen as a benefit.
- Migration of data and users had been straightforward.
- The council has assessed that it is achieving cost savings of approximately 60% (from a starting point estimated at £100 per user per year).

There have however been some challenges:

- It had been felt necessary to exclude users who require access to more sensitive information, meaning that the Lotus Notes system continues to be used in parallel with Google apps.
- Dual running of systems had caused some problems, for example coexistence of calendars.

Key learnings for future deployments include:

- Having a community wiki proved invaluable for enabling users to share solutions to initial problems in using Google apps, resulting in very few calls to the helpdesk.
- Having clearly set out process definitions and team structure information was critical to the migration process.

14.2.3 Hillingdon county council

Hillingdon have moved a number of their employees to Google apps from Microsoft products. They report that

- Most users were utilising only a small proportion of the Microsoft software suite.
- Implementation costs of Google apps were seen as “low”, with little training needed due to the familiar and intuitive user interface.
- Upfront planning and investment in self-help tools to provide support to users proved worthwhile.
- There have been benefits from productivity tools including collaboration.

Worthwhile cost reductions have been achieved, with cost reducing by 15-35% from the previous cost of the “on premise” solution (£255 per user per annum) to an estimated £216-£165 per user per annum.

14.2.4 Ordnance Survey

Ordnance Survey provide mapping graphics to a variety of websites; growth in use of the Internet has increased demand for these services which are subject to variable levels of demand.

Ordnance Survey utilise Amazon Web Services for serving requests for mapping graphics, and report that they benefit from the burstable, elastic service access. The ability to scale when required means that it is not necessary to invest in ICT infrastructure to handle peak load requirements, and development/test environments can be "turned off" when not needed. Cost savings compared to a conventional "on premise" approach are estimated to be in the region of 30%.

14.2.5 Government Digital Service (GDS)

GDS use a range of cloud services including Google apps. Significant cost savings are reported; over 80% for basic end-user computing, e-mail and office applications compared to the previous service that was provided by one of the major systems integrators. Agility is another benefit; for example an e-petitions service was delivered in eight weeks at a cost of £60,000.

In September 2012, GDS announced what at the time was the largest purchase through CloudStore to date; specifically the use of a infrastructure as a service product from Skyscape to host the new gov.uk site, an order valued at £600,000.

14.2.6 National Offender Management Service (NOMS)

In 2011 and 2012 NOMS ICT initiated a number of projects to assess the scope for using Cloud computing services to address business requirements at the National Offender Management Service:

14.2.6.1 Collaboration and CRM

In 2010, the agency decided to close an infrastructure platform called NOMSnet [55], which at the time supported around 2,000 users who were provided with desktops or laptops, e-mail and office software, access to the Internet, and hosted collaboration (SharePoint) and CRM (Microsoft dynamics) environments.

NOMSnet required extensive remedial work due to a building move and security deficiencies, and financial analysis indicated that significant cashable savings could be achieved by migrating

the NOMSnet user community to the Quantum system that is used by the majority of the agency's employees. (NB: Quantum is an integrated ICT system provided by HP;- it comprises a national secure private network, PCs and other devices in all prisons and HQ buildings, and national applications (eg for case management and offender risk assessment) that are hosted in HP data centres.)

The work was done in three phases:

- Phase 1: physically relocate the NOMSnet infrastructure to the new building.
- Phase 2: migrate the 2000 users to Quantum, opening new user accounts, providing laptops where required, migrating data (e-mail and files) from NOMSnet to Quantum, adding five additional desktop applications onto the Quantum applications catalogue, and recovery/recycling of the (by then obsolete NOMSnet) desktop and laptop PCs.
- Phase 3: identify alternative platforms for SharePoint and Microsoft Dynamics CRM, migrate the services and users, and decommission the NOMSnet infrastructure, ensuring secure storage of residual data (for archive purposes), and recovery/recycling of the hosting platform.

During phase 3, the UK Government CloudStore was used to identify alternative collaboration and CRM platforms. Huddle and Microsoft 365 CRM were identified as suitable public cloud services to which the NOMSnet users could be migrated.

One of the benefits of using of public cloud services is that the cost per user and the unit costs of the collaboration and CRM services is fully transparent; with NOMSnet the apportionment of cost would have been subject to assumptions on allocation of shared overheads and would thus have been open to challenge.

Hence, as part of the migration process, a decision was made to ask the head of each team using the services to cover the future cost of Huddle and Microsoft Dynamics CRM from his or her budget. This brought about a dramatic reduction in demand for the services and greater than expected savings. Specifically even though the new services were substantially cheaper, the request to cover the cost of the service saw over 80% of business sponsors deciding to discontinue their team's use of the service. The content of the discontinued services was securely archived using existing facilities, and thus reducing the ongoing cost of using Huddle and Microsoft 365.

The migration proceeded smoothly, with the only difficulty being with the service that was being migrated to Microsoft 365 CRM. A degree of expertise in migrating data into this CRM service was needed. Hence a third-party brokerage service was engaged to perform this task and to complete the production of the usage reports required by the business sponsor. The migration went smoothly, however production of reports took longer and required more resource than originally estimated. Much like a conventional ICT project, this demonstrates that cloud is no substitute for rigorous ICT planning, estimation and project management capability.

What the above cases have in common is that use of the Cloud computing service was predominantly to provide services to internal users, in cases where the commoditised service met the users needs “as is”, (i.e. where it was not necessary to integrate to a another back-end or front-end service to deliver the end-user need), and where the data involved was not highly sensitive.

14.2.7 Assessment of fit of Cloud computing services for “stand-alone” deployments

Table 7 overleaf depicts the fit of CloudStore services, in such “stand-alone” cases, against the assessment criteria set out at the start of Part 3:

Potential benefits of using Cloud computing services	Issues to be overcome
Cost reductions	The transition to Cloud computing services is inhibited by high costs and/or lack of skills needed skills for selecting, designing/securing, migrating data to, and managing Cloud computing services, and/or by legal/contractual constraints.
Accelerated innovation	Relationship imbalance; suppliers may be too big (or small) to take any individual customers needs/concerns into account
Meet consumers expectations in the mobile Internet era	Legal concerns over ability to assure compliance with rules on privacy, data residency etc
Increased choice and affordability of services for specialist needs	Lack of transparency of service design, security and management procedures
Flexibility to switch and scale use of services	Difficult to provide assurance that services meet their full specification
Dynamic supply marketplace to drive ongoing service improvement and cost reduction	Imperfect supply marketplace inhibits substitutability and thus price competition
Reduces risk by using well proven technology and suppliers	Information security risk – Inability to assure confidentiality, integrity and availability of services
	Inability to control future service characteristics
	Corporate governance frameworks unable to drive shift to Cloud computing, or ensure successful use of services and realisation of benefits
	Internal ICT organisations lack both the skills/culture for successful use of Cloud computing services, and the ability to build these for the future
	Overheads involved in selecting services proves prohibitive
	Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services
	The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive
	Some combination of the above undermines trust in business services that include a Cloud computing element

Table 7: Assessment or fit of public cloud services for "stand-alone" deployments that do involve use of sensitive data.: potential for delivering benefits and addressing obstacles to Cloud computing deployment

Code: Green -proposal addresses issue, Amber/Green – proposal largely addresses issue
Amber -- proposal partially addresses issue,
Amber/red -- proposal partially addresses issue but only in limited contexts,
Red -- proposal does not address issue. Blue – not applicable or not a significant issue

The conclusion from the table above is that it is already relatively easy to realise benefits from deployment of Cloud computing services where they are used for an internal user community (i.e. rather than for services that face off to customers), and where minimal integration (if any) is needed with existing internal services, and where data is not particularly sensitive. Most of the theoretical benefits of use of Cloud computing services can be realised in such cases, while the risks/obstacles either are not applicable, or become less relevant primarily because of the relative insensitivity of data.

14.3 Unsuccessful attempts to use G Cloud services for mission-critical applications

14.3.1 Deployment of public cloud services for a high-volume complex business process - Community Payback

Another attempt made by NOMS to deploy Cloud computing services was to underpin the business processes for Community Payback, which is one of the sentencing options available to the courts. Community Payback is a sentence where the offender is required to work a certain number of hours of unpaid work. It is a popular sentence and is a cheaper and more effective alternative to a short custodial sentence. Community Payback represents about 33% of the work of the Probation Service. Annually, around 70,000 offenders are sentenced, and work on in the region of 55,000 projects for a total of over 8 million hours.

Providing the information and business process enablement for Community Payback is relatively complex in that:

- community projects need to be sourced and scheduled.
- offenders need to be assigned to projects that are within reasonable travel time/distance of their homes.
- allocation of offenders to projects needs to take account of offenders' capability, background and risk profile to ensure a "suitable mix".
- project supervisors ideally need mobile devices on which they can access details of the offenders due on the project, and their history and risk profile, and also record details of work done.
- the probation trust needs to be able to evidence that offenders completed work on projects, and to maintain the offender case record (including case notes) for use both in subsequent discussions between offenders and probation officers, and for consideration when providing advice to courts in the event of any future offences.

In summer 2011, the intent was that provision of Community Payback sentences would transfer from the 35 probation trusts to 5 national private or public sector providers. It was decided to commission a study to assess whether use of Cloud computing service(s) would be a preferable means of providing the new providers with access to offender information and processes, as an alternative to adaptation of existing legacy systems.

The approach adopted was to invite four cloud providers to build "working prototypes" integrated with the existing test systems; these included:

- salesforce.com
- Microsoft 365 CRM
- Unilink Nforce (a system used by private sector prison operators) hosted on a secure private cloud provided by Savvis
- an existing case management system that has been developed in-house (CATS) hosted on Amazon Web Services

The prototypes, which were integrated with the legacy test database, showed that all four options could meet the documented functional requirements; i.e. use of Cloud computing services, either at the software as a service or infrastructure as a service levels, was technically feasible, and could meet the documented requirements.

Additionally, the public cloud services were able to provide valuable additional features, development of which through the conventional "in-house" model would have likely been excluded due to prohibitive cost and complexity.

The additional benefits that can be obtained include:

- mobile device access, where the public cloud services offered rich "out-of-the-box" integration with mobile devices, both for display of information and transactions.
- mapping services, that can be used both for allocation of offenders to projects nearby to their homes, as well as helping offenders and project supervisors find directions to the project's location.

A cost comparison was done over a ten-year period that indicated that the relative cost benefit from using cloud services varies, but that all but one of the four options was lower cost then the conventional "in-house" option (traditional design and build with specifically commissioned hosting). It is not surprising that use of Cloud computing services does not by itself guarantee cost reductions; assessment and analysis is needed on a case-by-case basis.

The median cost advantage of using the cloud services was approximately 50%, and the indications were that the cloud based service could be delivered within the business timescales. It was clear that using a "software as a service" platform was a better fit for this requirement then the "infrastructure as a service" options.

Given that Community Payback requires the exchange of large quantities of sensitive personal

data there was also careful consideration of risks. The questions that were asked included:

- Do we have the risk appetite for early adoption of a Cloud computing service taking into account unresolved security and information assurance concerns, the lack of a mature service management framework, the high profile and business critical nature of providing Community Payback services and the lack of experience in the retained ICT organisation and incumbent supplier base to successfully work with cloud service providers?
- Can our existing business case assessment framework be used to determine the best option?
- How do we determine the risks to successful delivery?
- Given that both of the "software as a service" providers have built global capabilities that will result in UK offender data travelling outside UK borders, is there confidence that data will not be compromised, that availability and integrity will be sustained, and that there would be no legal challenges?
- Can we be confident we can legitimately make and justify a decision to proceed with the cloud option given the above uncertainties?

In this case, there was not a clear way forward for resolving the above issues within a finite time scale. While there was support from senior levels for proceeding with a cloud option subject to business case and acceptable risk mitigation, in the event the need to be able to meet the business's timescale for implementation of the new delivery model resulted in the decision being made to proceed with a legacy/conventional approach to providing the ICT enablement, albeit this will potentially be at higher cost. In the time available it had not been possible to estimate the costs and timescales of overcoming the key risks involved in using CloudStore alternatives..

A key learning is that critical dependencies and the unresolved compliance questions rendered it impossible to commit to adopting the cloud solution in this case. Additionally the relative immaturity of current cloud adoption approaches means that the Community Payback project would have had to bear the cost of overcoming the above issues, meaning that for the budget holder the cloud option would in fact have ended up being a considerably more costly way forwards. Further information is available in a report authored by Adrian Scaife.

The table overleaf depicts the fit of the Community Payback case study against the assessment criteria set out at the start of Part 3:

Potential benefits of using Cloud computing services	Issues to be overcome
Cost reductions	The transition to Cloud computing services is inhibited by high costs and/or lack of skills needed skills for selecting, designing/securing, migrating data to, and managing Cloud computing services, and/or by legal/contractual constraints.
Accelerated innovation	Relationship imbalance; suppliers may be too big (or small) to take any individual customers needs/concerns into account
Meet consumers expectations in the mobile Internet era	Legal concerns over ability to assure compliance with rules on privacy, data residency etc
Increased choice and affordability of services for specialist needs	Lack of transparency of service design, security and management procedures
Flexibility to switch and scale use of services	Difficult to provide assurance that services meet their full specification
Dynamic supply marketplace to drive ongoing service improvement and cost reduction	Imperfect supply marketplace inhibits substitutability and thus price competition
Reduces risk by using well proven technology and suppliers	Information security risk – Inability to assure confidentiality, integrity and availability of services
	Inability to control future service characteristics
	Corporate governance frameworks unable to drive shift to Cloud computing, or ensure successful use of services and realisation of benefits
	Internal ICT organisations lack both the skills/culture for successful use of Cloud computing services, and the ability to build these for the future
	Overheads involved in selecting services proves prohibitive
	Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services
	The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive
	Some combination of the above undermines trust in business services that include a Cloud computing element

Table 8: Implemented G Cloud strategy: potential for delivering benefits and addressing obstacles to Cloud computing deployment for moderate complexity 'end user' services
Code: Green -proposal addresses issue,
Amber proposal partially addresses issue,
Amber/red proposal partially addresses issue but only in limited contexts,
Red proposal does not address issue.

14.3.2 Using Cloud computing services to substitute for a failing case management project deployment

An unsuccessful attempt was made to use G Cloud services as an alternative supply route for provision of a new case management system for the probation service following slippage on an existing project. This failed as the main challenge was migrating data from legacy systems to the a new national database;- while cloud services could have met the users needs, they did not provide a faster route for data migration, and indeed introduced new issues of control and security of data once migrated.

The table below depicts the fit of the Case Management system against the assessment criteria set out at the start of Part 3:

Potential benefits of using Cloud computing services	Issues to be overcome
Cost reductions	The transition to Cloud computing services is inhibited by high costs and/or lack of skills needed skills for selecting, designing/securing, migrating data to, and managing Cloud computing services, and/or by legal/contractual constraints.
Accelerated innovation	Relationship imbalance; suppliers may be too big (or small) to take any individual customers needs/concerns into account
Meet consumers expectations in the mobile Internet era	Legal concerns over ability to assure compliance with rules on privacy, data residency etc
Increased choice and affordability of services for specialist needs	Lack of transparency of service design, security and management procedures
Flexibility to switch and scale use of services	Difficult to provide assurance that services meet their full specification
Dynamic supply marketplace to drive ongoing service improvement and cost reduction	Imperfect supply marketplace inhibits substitutability and thus price competition
Reduces risk by using well proven technology and suppliers	Information security risk – Inability to assure confidentiality, integrity and availability of services
	Inability to control future service characteristics
	Corporate governance frameworks unable to drive shift to Cloud computing, or ensure successful use of services and realisation of benefits
	Internal ICT organisations lack both the skills/culture for successful use of Cloud computing services, and the ability to build these for the future
	Overheads involved in selecting services proves prohibitive
	Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services
	The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive
	Some combination of the above undermines trust in business services that include a Cloud computing element

Table 9: Implemented G Cloud strategy: potential for delivering benefits and addressing obstacles to Cloud computing deployment for high complexity/sensitivity 'end user' services
Code: Green -proposal addresses issue, Amber - proposal partially addresses issue, Amber/red - proposal partially addresses issue but only in limited contexts, Red - proposal does not address issue.

14.4 Procuring "mission critical" government ICT in 2012/13

The Ministry of Justice Is one of seven government departments that handles the majority of citizen transactions, and has been selected as a pioneer for G Cloud on the basis that the majority of its existing contracts expire from 2014. With approximately 100,000 employees the ministry purchases ICT at large scale, with total ICT spend (in 2013) being in the order of £500 million per annum.

MoJ needed to determine its future ICT sourcing strategy in early 2011, when it considered it unlikely that the G Cloud suppliers would be able to successfully take on all the current ICT

infrastructure and applications portfolio. Hence MoJ decided to embark on a parallel procurement path, initiating a programme named “Future IT Supply” (FITS).

In addition, MoJ has continued to support the G Cloud programme, being one of the leading departments in sourcing services from CloudStore where they represent a good match for new business requirements [56]. However the decision by MoJ to embark on the parallel FITS procurement exercise for its strategic ICT supply effectively meant that its initial purchases from the G Cloud programme would be of relatively small-scale. For the future, there is a key opportunity to encourage the FITS suppliers to repackage the services being implemented for MoJ as G Cloud services, and to make these available as private cloud services on the CloudStore for use by other governmental organisations.

The table overleaf compares the MoJ Future ICT Sourcing Strategy against the assessment criteria set out at the start of Part 3:

Potential benefits of using Cloud computing services	Issues to be overcome
Cost reductions	The transition to Cloud computing services is inhibited by high costs and/or lack of skills needed skills for selecting, designing/securing, migrating data to, and managing Cloud computing services, and/or by legal/contractual constraints.
Accelerated innovation	Relationship imbalance; suppliers may be too big (or small) to take any individual customers needs/concerns into account
Meet consumers expectations in the mobile Internet era	Legal concerns over ability to assure compliance with rules on privacy, data residency etc
Increased choice and affordability of services for specialist needs	Lack of transparency of service design, security and management procedures
Flexibility to switch and scale use of services	Difficult to provide assurance that services meet their full specification
Dynamic supply marketplace to drive ongoing service improvement and cost reduction	Imperfect supply marketplace inhibits substitutability and thus price competition
Reduces risk by using well proven technology and suppliers	Information security risk – Inability to assure confidentiality, integrity and availability of services
	Inability to control future service characteristics
	Corporate governance frameworks unable to drive shift to Cloud computing, or ensure successful use of services and realisation of benefits
	Internal ICT organisations lack both the skills/culture for successful use of Cloud computing services, and the ability to build these for the future
	Overheads involved in selecting services proves prohibitive
	Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services
	The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive
	Some combination of the above undermines trust in business services that include a Cloud computing element

Table 10: Implemented G Cloud strategy: potential for delivering benefits and addressing obstacles to Cloud computing deployment for MoJ wide ICT services
Code: Green -proposal addresses issue,
Amber proposal partially addresses issue,
Amber/red proposal partially addresses issue but only in limited contexts,
Red proposal does not address issue.

The FITS programme is sourcing new ICT suppliers in the following categories:

- End user computing
- Networks
- Hosting
- Application maintenance and support
- Service integration and management.

By consolidating demand across MoJ, and purchasing ICT in categories for which benchmarking data is available, MoJ assesses it is on target to achieve savings of approximately 30% on current pricing levels (reducing annual costs from £500 million pa to £350 million pa).

14.5 Hybrid cloud proposal - pan government hosting framework

A cross government initiative to create a “pan government hosting framework” was discontinued following a review of procurement policy. One of the bids on this framework had been from a consortium that appeared to offer a strong “Hybrid cloud” combination of:

- Creation of a highly efficient commodity cloud hosting facility on the UK mainland.
- Partnering with a leading operator of “legacy capable” data centres.
- Funded by private equity.
- The intent to initially migrate 30 to 50% of Ministry of Justice workload to the cloud hosting platform.
- A plan to engage a network of SME software development organisations to replatform “hard to migrate” applications from the “legacy capable” datacentre to the “commodity cloud” facility, doing so:
    - Using a services orientated architecture model, creating a common platform with shared services for identity management, payments etc, and
    - Using the savings achieved on applications hosting costs to fund additional migrations, with
    - Initial funding of up to £1 billion provided by the private equity firm.

The table overleaf depicts the fit of this proposal for the pan government hosting framework against the assessment criteria set out at the start of Part 3:

Potential benefits of using Cloud computing services	Issues to be overcome
Cost reductions	The transition to Cloud computing services is inhibited by high costs and/or lack of skills needed skills for selecting, designing/securing, migrating data to, and managing Cloud computing services, and/or by legal/contractual constraints.
Accelerated innovation	Relationship imbalance; suppliers may be too big (or small) to take any individual customers needs/concerns into account
Meet consumers expectations in the mobile Internet era	Legal concerns over ability to assure compliance with rules on privacy, data residency etc
Increased choice and affordability of services for specialist needs	Lack of transparency of service design, security and management procedures
Flexibility to switch and scale use of services	Difficult to provide assurance that services meet their full specification
Dynamic supply marketplace to drive ongoing service improvement and cost reduction	Imperfect supply marketplace inhibits substitutability and thus price competition
Reduces risk by using well proven technology and suppliers	Information security risk – Inability to assure confidentiality, integrity and availability of services
	Inability to control future service characteristics
	Corporate governance frameworks unable to drive shift to Cloud computing, or ensure successful use of services and realisation of benefits
	Internal ICT organisations lack both the skills/culture for successful use of Cloud computing services, and the ability to build these for the future
	Overheads involved in selecting services proves prohibitive
	Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services
	The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive
	Some combination of the above undermines trust in business services that include a Cloud computing element

Table 11: Pan government hybrid cloud proposal: potential for delivering benefits and addressing obstacles to Cloud computing deployment for high complexity/sensitivity 'end user' service

Code: Green -proposal addresses issue,
Amber proposal partially addresses issue,
Amber/red proposal partially addresses issue but only in limited contexts,
Red proposal does not address issue.

14.6 Chapter conclusion

By 2013 G Cloud has become well established as a new government ICT procurement route that allows for more rapid sourcing of many ICT services. It is most readily used for services that are not business critical, that do not involve sensitive data, and that do not require significant integration with other services. At present it is complex and costly to use combinations of G Cloud services to create secure "line of business" processes, and this is restricting adoption of G Cloud in many cases.

The table below provides a consolidated view of the assessments of cloud fit provided earlier in Section 3. This is followed by an "ease of fit' ranking of the usage scenarios (best fit to worst fit), and an a frequency of occurrence ranking of the underlying obstacles (ranked by category and individually). These rankings are then used in Chapter 16 to support identification and prioritization of the services to be provided by cloud services brokerages.

Potential benefits of using Cloud computing services	Proposed G Cloud Authority	G Cloud strategy	Stand alone services	Moderate complexity	High complexity	Ministry ICT re-procurement	Hybrid cloud proposal
Cost reductions							
Accelerated innovation							
Meet consumers expectations in the mobile Internet era							
Increased choice and affordability of services for specialist needs							
Flexibility to switch and scale use of services							
Dynamic supply marketplace to drive ongoing service improvement and cost reduction							
Reduces risk by using well proven technology and suppliers							
Issues to be overcome -- Transition							
Transition inhibited by high costs/lack of skills needed for designing/securing, migrating data to, and managing Cloud computing services, and/or by legal/contractual constraints.							

Potential benefits of using Cloud computing services	Proposed G Cloud Authority	G Cloud strategy	Stand alone services	Moderate complexity	High complexity	Ministry ICT re-procurement	Hybrid cloud proposal
Issues to be overcome -- Buyer confidence							
Relationship imbalance; suppliers may be too big (or small) to take individual customers needs/concerns into account							
Legal concerns over ability to assure compliance with rules on privacy, data residency etc							
Lack of transparency of service design, security and management procedures							
Difficult to provide assurance that services meet their full specification							
Imperfect supply marketplace inhibits substitutability and thus price competition							
Issues to be overcome – Compliance							
Information security risk – Inability to assure confidentiality, integrity and availability of services							
Inability to control future service characteristics							
Issues to be overcome – Buyer capability							
Corporate governance frameworks unable to drive shift to Cloud computing, or ensure successful use of services and realisation of benefits							

Potential benefits of using Cloud computing services	Proposed G Cloud Authority	G Cloud strategy	Stand alone services	Moderate complexity	High complexity	Ministry ICT re-procurement	Hybrid cloud proposal
Internal ICT organisations lack both the skills/culture for successful use of Cloud computing services, and the ability to build these for the future							
Overheads involved in selecting services proves prohibitive							
Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services							
The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive							
Issues to be overcome – User trust							
Some combination of the above undermines trust in business services that include a Cloud computing element							

Table 12: Consolidated assessments of ability of cloud usage scenarios to deliver benefits and overcome obstacles

The options have been ranked using the scoring system indicated in the table below. Amber has been considered to be a neutral rating, with blue, green and amber/green ratings scoring positively, while amber/red and red ratings score negatively.

Potential benefits of using Cloud computing services (score)	Proposed G Cloud Authority	Hybrid cloud proposal	Stand alone services	Moderate complexity	High complexity	Ministry ICT re-procurement	G Cloud strategy
Blue/Green (10)	21	11	6	5	5	6	
Amber/Green (5)		5	3				1
Amber (0)		2	3	4	3	1	5
Amber/Red(-5)		3	8	4	2		7
Red (-10)			1	8	11	14	8
Criteria check	21	21	21	21	21	21	21
Score=	210	120	15	-50	-70	-85	-110
Ranking	1 (top)	2	3	4	5	6	7

Table 13: Ranked fit of deployment scenarios to benefits and obstacles

From this analysis, the ranking of the options assessing the practicality of using Cloud computing services for line of business applications is as follows:

Figure 7: Ranking of Cloud computing deployment options

Positive Scores – benefit of using cloud likely to justify overheads

- G Cloud Authority (best fit)
- Hybrid cloud proposal
- Use of CloudStore for stand-alone services

Negative Scores – benefit of using cloud unlikely to justify overheads

- Use of CloudStore for moderate complexity services
- Use of CloudStore for high complexity services
- Use of CloudStore for replacing all Ministry of Justice ICT
- Published G Cloud strategy (most gaps)

From the above assessments, the frequency of occurrence of factors that need to be addressed to enable routine use of Cloud computing services have been ranked, as follows:

A. By category

- Demonstrating **compliance** with legal and security requirements (greatest challenge)
- Establishing confidence that Cloud computing buyers can maintain **control** of their business information services when using Cloud computing services, that services can be assured and that suppliers will not exploit their power in the future

- Establishing **trust** amongst users of Cloud computing services
- Building buyer **capability** to manage selection, transition and service providers
- **Initiation** of Cloud computing based projects (less challenging)

B. By issue:

Issue	Net score
Lock-in, with an imperfect supply marketplace inhibiting substitutability and thus price competition	-45
Information security risk; inability to assure confidentiality, integrity and availability of services	-35
Difficult to provide assurance that services meet their full specification	-30
Lack of transparency of service design, security and management procedures	-25
Unacceptable levels of risk are created by migrating existing "business critical" services from legacy to Cloud computing services	-20
The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive	-20
Corporate governance frameworks are unable to drive shift to use of Cloud computing, or to ensure successful use of services and realisation of benefits	-20
The overheads involved in selecting Cloud computing services proved prohibitive	-20
Some combination of the issues listed undermines trust in business services that include a Cloud computing component	-20
Legal concerns over ability to assure compliance with rules on privacy, data residency etc	-15
Internal organisations lack the skills/culture for successful use of Cloud computing services, and are unable to build these	-15
Transition to Cloud computing services is inhibited by high costs/lack of skills needed for designing, securing, migrating data to and managing Cloud computing services, or by legal/contractual constraints	-10
Relationship imbalance; suppliers may be too big (or too small) to take individual customers needs/concerns into account	-5

Table 14: Ranking of obstacles to cloud deployment (more negative = greater impact)

Experience in the period 2011 to 2013 is consistent with the conclusions from the analysis that is set out above. As described earlier most progress has been made with deploying cloud services where the commodity service meets the business needs on an “as is” basis, with relatively little need for integration with sensitive internal data. By mid 2013 very limited progress has been made with the “line of business” services that account for the majority of current ICT spend, which require both combinations of services and secure handling of sensitive data.

Part 4: Cloud Computing in UK Government – Overcoming barriers to deployment and next steps

Chapters 15 considers the successes and gaps in the work completed to date, reviews whether in light of experience the cloud opportunity is still worth progressing, and identifies the actions, benefits and risks involved in making continued progress.

Chapter 16 sets out how Cloud services brokerages, acting as an intermediary between the provider and buyer of Cloud computing services, can potentially share the cost of risk mitigation between multiple organisations. They can therefore accelerate the point at which it becomes viable to migrate existing conventional ICT solutions to the Cloud computing model.

15.0 Assessment of G Cloud programme to date

15.1 Context

There is no question that the G Cloud programme has begun to achieve the potential benefits that were envisaged in 2010. This is evidenced by the sales information reported in section 14.1.

The key obstacle still to overcome is the successful and secure use of combinations for Cloud computing services to underpin the mission specific 'line of business' services that account for the majority of large organisations' ICT spend.

15.2 Barriers to Cloud computing deployment in UK government

The major factors that are inhibiting the transition of the UK public sector to the use of Cloud computing services are:

- Risks anticipated in 2010 and 2011 (Sections 11.5.4 and 13.4).
- Change in government policy, resulting in less investment/commitment both by suppliers in creating services suitable for use by government departments, and by departments in selecting alternative services (Section 12.3).

These are described below:

a. Risks

To varying extents, all the risks that were envisaged when the business case was written in 2010 have come to pass, as set out in the table below: -

Risk envisaged in 2010	Outturn as at June 2013
Lack of funding for initiating the programme.	Programme did not receive funding beyond the minimum necessary to establish CloudStore
Failure to secure senior stakeholder buy in may inhibit service take-up.	Incoming government had multiple political ambitions for ICT beyond cost reduction. The G Cloud programme was repositioned to add a major objective of opening up purchases from SMEs
The G Cloud Authority (internal cloud services broker) does not receive the empowerment and authority needed to drive implementation with public sector	G Cloud Authority has not been funded; thus has not been created and is unable to drive progress.

organisations.	
Stakeholder management is not sufficiently effective to bring together currently duplicative procurements and other processes.	To a significant extent due to the issues set out above, the G Cloud programme did not establish early momentum for providing suitable secure services for business critical ICT provision, as assessed for example by the Ministry of Justice when embarking in FITS.
The programme does not demonstrate sufficient cashable savings to secure ongoing funding.	Cashable savings identified in the 2010 business case were seen as insufficient to justify allocation of funding at a time of austerity.
The pressure for cost reduction is such that the pricing and other commercial terms imposed on suppliers is insufficient to justify the necessary supplier investment in achieving transition.	Suppliers have been asked to achieve short-term cost reductions through reducing margins. Suppliers have been slow to invest in government specific services in the absence of a clear migration plan to move away from use of legacy ICT. However around 20 secure services are now available.
ICT suppliers undermine the programme by building momentum for proprietary "cloud" services that inhibit achievement of programme objectives.	There are not (as of 2013) agreed standards for describing cloud services, for migrating data or for achieving interoperability. Hence the industry is currently providing a series of "islands of Cloud computing capability" and although all of these are connected at the TCP/IP level, client specific investment is needed to achieve business interoperability.

Table 15: 2013 outturn on risks envisaged by G Cloud programme team in 2010

b. Changes in government policy

Additionally Ministers have set new objectives for government ICT to utilise open source code, open standards, and SMEs. These expectations conflict with the most direct path to realising early benefits from Cloud computing, which is most quickly achieved by establishing a (large scale) shared private Cloud computing capability for business critical citizen facing services.

Parallel directional pressure has come from the government security and legal communities, where there is concern about the legality of citizen data being held (or transiting) 'off-shore', and about the potential for other governments' agencies to access data held within the major cloud providers (for example in the US using the provisions under the Patriot Act).

Additionally other government initiatives, including the focus on a business transformation based approach to modernising public services under the 'digital by default' policy, and the pressure on incumbent suppliers to deliver immediate cost savings through reducing margins, have diluted the focus on transitioning existing services to Cloud computing.

Hence the additional risks identified when the Government Cloud strategy was published in 2011 have also become issues, as set out in the table below:

Additional risk envisaged in 2011	Outturn as at May 2013
Leadership, specifically the challenge of aligning the G Cloud and data centre consolidation with the other major elements of the government ICT strategy.	Responsibility for leading the G Cloud initiative has been allocated (as an additional responsibility) to senior government ICT practitioners, supported by a relatively small number of staff. As a result, there has not been the leadership bandwidth to address the more complex aspects of the changes required, ie those that need to be addressed to yield the biggest benefits.
Internal delivery capability, including availability of skills and knowledge needed to successfully deliver in the new environment, moving the prevailing "mindset" from "let's build another new solution" to "let's reuse what we've got", achieving effective end to end service management when using commodity multi tenanted cloud services that are shared between many organisations, and introducing an effective and efficient information assurance regime for public and private G Cloud services.	Minimal resources have been allocated to driving change at the 'ICT practitioner' level; as a result there is neither a clear medium term strategy for transitioning existing ICT services to Cloud computing services, nor for building the skills and advisory and support services needed to do so effectively.
Market/supplier response, with there being recognition that it's essential for the supplier marketplace to view the provision of G Cloud services as an attractive business proposition, given the need for upfront investment to make G Cloud services available on a "pay as you use" basis.	SMEs in general have responded well, viewing CloudStore an opportunity to supply to government for the first time. Existing suppliers have now begun to introduce some cloud services into the CloudStore. Larger consumer focused cloud suppliers have however viewed even the potential of business from across UK government as being insufficient to justify their investment in dedicated resource to flex services, the information disclosed, and commercial terms etc to meet government requirements.

Table 16: 2013 outturn on risks envisaged in published G Cloud strategy (2011)

The above risk assessment is consistent with surveys of Government ICT practitioners which have reported that Cloud computing is seen as being 'high risk', and that this is slowing uptake. The top concerns ([32],[33],[35]) that are reported as delaying adoption of Cloud Computing services are (inadequate data) security, perceived risks from using "unproven" technology, lack of confidence/control of data residency, and lack of a framework for building the business case.

This is despite public sector organisations acknowledging benefits such as flexibility, agility, lower costs and improved service levels from using cloud services.

15.3 Authors perspective on barriers

The authors experience reinforces the issues identified above. This is informed in part by both experience, and by practitioner interviews and conversations conducted in the period 2009 to 2012. The following concerns have repeatedly surfaced:

15.3.1 Security concerns

Security concerns are consistently cited as the top issue. Where a service is “mission critical” to an organisation, compared to the conventional “on premise” approach, use of cloud services creates new risks such as loss of data, complete loss of the business service, inability to influence future direction of the service thus rendering ICT unable to meet the needs of the business, and legal non-compliance, for example should personal data unknowingly be accessed outside the home country. Specific concerns include the following:

- some public cloud providers have had reported data losses.
- others have had significant compromises.
- one large-scale public cloud provider while committing to hosting data in the EU, acknowledges that it is possible that a support call would be picked up in Asia, and that the operative will then potentially have access to customer data needed to resolve the fault ticket.
- security risks have inhibited deployment of cloud services to users with a need for access to more sensitive data.

15.3.2 Legal issues

Lack of clarity on legal issues is also a top concern.

Public cloud providers have commoditised technology platforms that are logically identical in all countries. Yet different countries apply different rules. Concerns include:

- Data protection; if personal data is accessed in another country, even for a support call, does this require explicit permission from the data subject?

- Freedom of information; where organisations are obliged to respond to requests to disclose information held on particular topics and subjects, can cloud providers be relied upon to retain critical information for the statutory retention period, even though this period may be set by a different jurisdiction? Of course this issue can be managed by the consumer of cloud services, but with additional overhead.
- Government disclosure obligations; for example if a US government agency used the Patriot Act to oblige a US based cloud services provider to disclose information on a UK citizen, who is liable if a UK court determines there has been a breach of the Data Protection Act or other legislation? What is the implication if a law enforcement authority confiscates a disk drive that holds data for multiple organisations?

15.3.3 Network risks

Use of Cloud computing services depends entirely on there being reliable and performant network access from the user's location to the cloud services provider. This requires higher levels of network resilience in many cases. One of the key features of cloud is dynamic scalability; this of course may impose higher peak loads on networks. The concept of "on demand scalability" has not generally been adopted by network providers, and this thus creates a potential "pinch point".

15.3.4 Service management

Cloud service providers usually infer the promise of "infinite scalability on demand". Yet this promise cannot be delivered. Some cloud providers provide the physical capacity to be able to sustain this promise in say 99.9% of cases. Others invest to a lower level. All offer only a limited financial guarantee promising reimbursement of some portion of service costs, without accepting any consequential liability. Yet for an organisation committing to use cloud services it's essential that critical business needs are underpinned with genuine physical provisioning. There is also the risk of exceptional situations such as the Olympics, or the London riots, meaning that peak load coincides across different user communities, and potentially within an essential business delivery period.

Specifically (in 2013) cloud service management methodologies and tooling cannot guarantee the end-to-end service predictability (particularly for complex business processes) that is attainable with established enterprise ICT approaches. These impacts are multiplied where

several cloud services need to be used in combination.

15.3.5 Architecture and design

Using cloud services successfully, particularly for more complex business processes requires additional skills such as:

- architectural techniques that take advantage of the new capabilities available through a cloud approach, i.e. “cloud aware design”.
- design for elasticity at the data, transaction and service levels.
- WAN design that is integrated with cloud service design; from the perspectives of resilience, security etc

15.3.6 Governance frameworks

Use of cloud services offers ever greater choice, and opens the potential for more ICT sourcing decisions to be made at the business unit, or even the end-user levels. Yet unconstrained choice is also a recipe for chaos! The ultimate goal for Chief Information Officers is to enable “high value added use of business information”.

However, if used across an organisation in an unconstrained manner, Cloud computing can intensify the fragmentation of an organisation’s information assets, thus destroying business value. Hence a governance approach is needed that is simultaneously supportive of local innovation while enabling sustained coherence of information assets at the organisational level. It is not yet clear how best to strike this balance.

Specific issues to consider include:

- In-house capability; addressing the above requires in-house teams that have relevant understanding, skills and experience, and which thus have demonstrable competence in using cloud services to address organisational ICT needs. In the main these capabilities are still at an early stage of development; while in most organisations there will be some “enthusiastic early adopters”, as of mid 2013 there is not in the main the experience to use cloud services, particularly public cloud services, for large-scale mission-critical processes.

- Standards; while some standards are readily adopted by all cloud providers (e.g. web standards such as IP and HTTP), there is not consistency in approaches in areas such as:
  - capacity management.
  - service management.
  - service provisioning.
  - data standards.
  - cloud bursting etc.

  While a framework such as ITIL 3 could be adapted to enable management of hybrid services consisting of public and private cloud services as well as in-house services, organisations will need to consider how to extend the framework and implement such an approach. Standards for application level interoperability between clouds are further away, although the IEEE is undertaking work in this area.

In theory, if a complete set of standards were in place, selection of cloud services could be done automatically and dynamically, in some cases without the end-user even being aware. While the US National Institute for Standards and Technology (NIST) has announced the intention to develop a range of standards to achieve outcomes such as the above [61], this work is at an early stage and is not generally adopted today by public cloud providers. In the absence of this, more manual "case-by-case" work is needed both to integrate cloud services, and to effectively use a portfolio of services.

Understanding and managing the various characteristics of a portfolio of selected services requires investment (money and time). This in turn creates an "entry barrier" that is restricting adoption.

15.3.7 Cost predictability

There are various indications in the savings estimates that producing a definitive cost comparison between Cloud computing and existing approaches is complex as it is not a "like-for-like" comparison, with the actual future cost of cloud services being subject to more variability as it is dependent on usage, and vendors' future pricing changes.

15.3.8 Business leaders risk appetite.

Given the risk context outlined above, it is perhaps not surprising that business leaders in many large organisations are currently not supportive of transitioning core enterprise ICT to Cloud computing services. This again points to a phased transition approach, to be underpinned by a "benefits roadmap" that enables experience to be gained from relatively low risk deployments, and a "capability building" roadmap to be put in place so that the usage footprint can build over time.

15.4 Cloud computing industry developments

The consumer focused Cloud computing industry goes from strength to strength. Organisations such as Amazon Web Services, Google Enterprise and salesforce.com are reporting strong growth rates and a growing number of clients that are comparable in scale to government departments.

These large-scale Cloud computing providers are innovating rapidly, with applications platforms such as those provided by Microsoft, Google and salesforce.com enabling accelerated business innovation for the delivery of highly functional services. These can be accessed on mobile devices as well as conventional PCs. In parallel infrastructure platforms such as those provided by Amazon Web Services, RackSpace and again Google and Microsoft are growing rapidly, offering highly attractive pricing that is enabled by the very high hardware utilisation levels that are being achieved.

15.5 Chapter conclusion -- the UK government is already realizing significant benefits from using Cloud computing services; benefits can be enhanced through persisting with efforts to utilise shared cloud services for citizen facing "line of business" processes.

As can be seen from earlier chapters, progress is being made with the UK public sector's use of Cloud computing services in areas where both the use of ICT is relatively straightforward (i.e. for "single function" activities that can be deployed on a relatively stand-alone basis), and where the standards of protection needed from the information assurance perspective are relatively low (e.g. citizen facing websites rather than core case management applications).

The solid foundations now established need to be extended from addressing "relatively straightforward" business needs, to begin to address the "core line of business processes" that

represent the essence of most organisations' information processing. Specific areas where additional capabilities are needed include:

- Building the capability, and facilitating the "cultural/ways of working" change needed for the government ICT profession to embrace cloud services.
- Putting in place a leadership framework to progressively build momentum.
- Establishing the link between deployment of Cloud computing services, and progressive rationalisation of the existing data centre estate.
- Accelerating the "foundation delivery partner programme", to build momentum in the adoption of "exemplar" cloud services by high-profile "first user" public sector organisations, thus providing leadership that others will follow.
- Establishing the G Cloud Authority with the power to set standards and mandate public sector organisations to deploy cloud services.
- Putting in place a planned migration programme to migrate from existing services to use cloud services, doing this in the context of a "commissioning and adoption roadmap".
- Putting in place a service management framework that allows combinations of cloud services to be used to achieve business process outcomes with predictable and consistent performance, availability and security.

Realistically, with the next UK election now being less than two years away, government ICT policies for this Parliament are now set, and the earliest change in approach, strategy or investment levels will be in 2015.

Meanwhile there is growing momentum to use Cloud computing services across UK government, and the benefits that were originally anticipated from a transition to Cloud computing are beginning to be attained. The next chapter considers what actions should be taken to accelerate benefits realisation.

In summary the significant developments since the G Cloud business case was produced in 2010 are:

- The major (US Silicon Valley based) cloud providers have continued to innovate, extending their breadth of services, and reducing prices.
- Similar UK based cloud providers have not gained comparable scale (although there is an ever-growing range of providers, comprising a complete spectrum of large, medium and small organisations).
- The G Cloud brand now has a valuable reputation, and has proven that significant cost

reductions can be delivered. It has not yet however demonstrated that it can provide the full range of capabilities to underpin business critical, citizen facing process delivery as had been envisaged in 2010.

- The G Cloud programme has not been funded to proceed beyond a procurement exercise, and basic accreditation of services.

The benefits from using Cloud computing services remain attractive, but given the impracticality of individual departments overcoming the many hurdles on a project by project basis, and the incentives of current suppliers to maintain the status quo, benefits delivery will remain below potential unless there is a collaborative campaign to drive adoption, preceded by strategic procurement of the necessary enabling services.

16.0 Cloud services brokerage

16.1 Context

Chapter 14 considered the work done within the UK government to date on Cloud computing, and identified the circumstances in which it is now possible to deploy Cloud computing successfully, as well as the constraints that are inhibiting ubiquitous use for citizen facing services. An assessment was provided of the fit of the alternative deployment approaches; this concluded that as at July 2013, other than for relatively simple deployments, the overheads of deploying Cloud computing services in medium or high complexity cases will in many cases exceed the benefits. This was summarised in Table 7 (repeated) below.

Figure 7: Ranking of Cloud computing deployment options

Positive Scores – benefit of using cloud likely to justify overheads	• G Cloud Authority (best fit) • Hybrid cloud proposal • Use of CloudStore for stand-alone services
Negative Scores – benefit of using cloud unlikely to justify overheads	• Use of CloudStore for moderate complexity services • Use of CloudStore for high complexity services • Use of CloudStore for replacing all Ministry of Justice ICT • Published G Cloud strategy (most gaps)

As discussed at the start of part three of this thesis, the "G Cloud Authority" based approach proposed in 2010 would have addressed the barriers that have subsequently been encountered as public sector organisations have sought to adopt Cloud computing services.

Chapter 14 also identified five categories of the issues/barriers that need to be overcome to drive up deployment of Cloud computing services in more complex business process scenarios, as follows:

1. Demonstrating **compliance** with legal and security requirements (greatest challenge)
2. Establishing confidence that Cloud computing buyers can maintain **control** of their business information services when using Cloud computing services, that services can be assured and that suppliers will not exploit their power in the future

3. Establishing **trust** amongst users of Cloud computing services
4. Building buyer **capability** to manage selection, transition and service providers
5. **Initiation** of Cloud computing based projects (less challenging)

Chapter 15 considered the organisational and policy issues that have shaped the government's approach to the G Cloud programme. It concluded that the barriers to adopting Cloud computing services for "mainstream" government ICT are substantive, and that without directed effort these barriers will not quickly erode over time. It is also clear that the coalition government in 2010 had multiple objectives for ICT, including opening up opportunities for SMEs and driving down ICT costs in pursuit of the austerity programme.

Nevertheless, the growing range of security accredited services available via the CloudStore does mean that there is still the opportunity to pursue adoption for the line of business processes discussed throughout this thesis. Realistically doing so will that require combinations of services are integrated with internal data assets, and delivered in a manner that inspires confidence that security and service requirements will also be met. The services to enable such outcomes can potentially be delivered by specialist intermediaries known as cloud services brokerages. This chapter (chapter 16) sets out the resulting opportunity for the establishment of cloud services brokerages.

16.2 What services will cloud services brokerages needs to provide to help their clients overcome barriers to deployment?

The chart below depicts the services that client services brokerages can potentially provide to address each of the categories of deployment obstacle set out earlier. Further information on each of the proposed services is provided in the following sections.

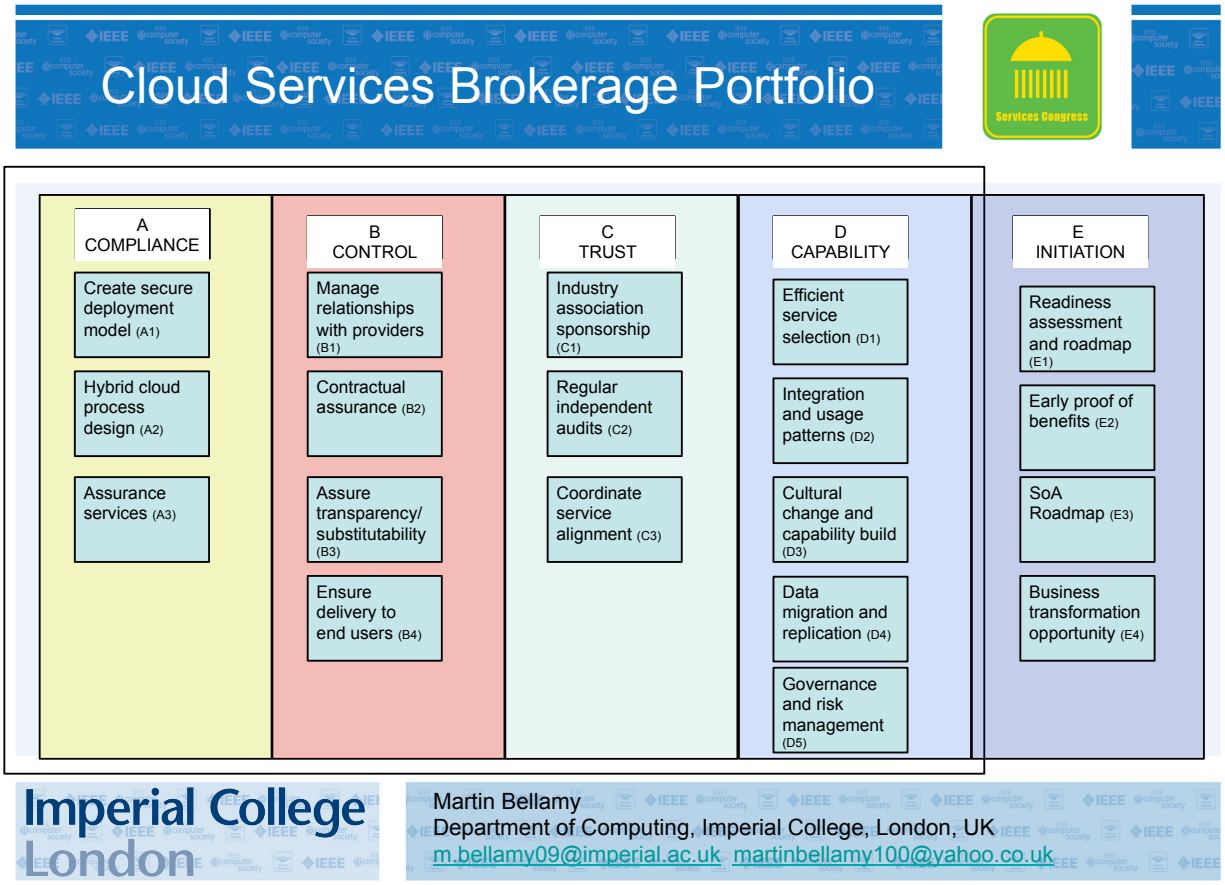


Figure 8: Cloud Services Brokerages – Potential Services

16.2.1 Compliance with business requirements, security and audit requirements

To support their customers in demonstrating compliance, cloud services brokerages will require an auditable framework to demonstrate that design, implementation and management practices for cloud-based solutions are sound. They will also need to work with their customers to ensure that their designs can be integrated with the client's enterprise architecture, as well as providing assurance that the combined solution will be auditable [63].

16.2.1.1 Creating a secure deployment model (A1)

Providing assurance of compliance with information security (confidentiality, integrity and availability) requirements, and that services meet their specifications in full, and will not change in a way that inconveniences the customer organisation requires either that:-

a. Cloud services brokerages have significant market power, and can be confident of

exerting influence over the cloud providers (unlikely in most cases due to the very large scale of the leading Cloud computing providers), or,

b. The cloud services brokerage selects or commissions only services that meet security requirements, or
c. The cloud services brokerage is able to use a range of cloud services in a way that limits the risks of compromise, disruption or failure of any single provider,
d. A suitable combination of the above.

For example, an approach to achieve the option c above is a "three level" approach that allows a range of different (potentially insecure) cloud services to be used in a manner that limits dependence on any specific cloud provider.

This is depicted in the diagram below, and described in the following sections:

.

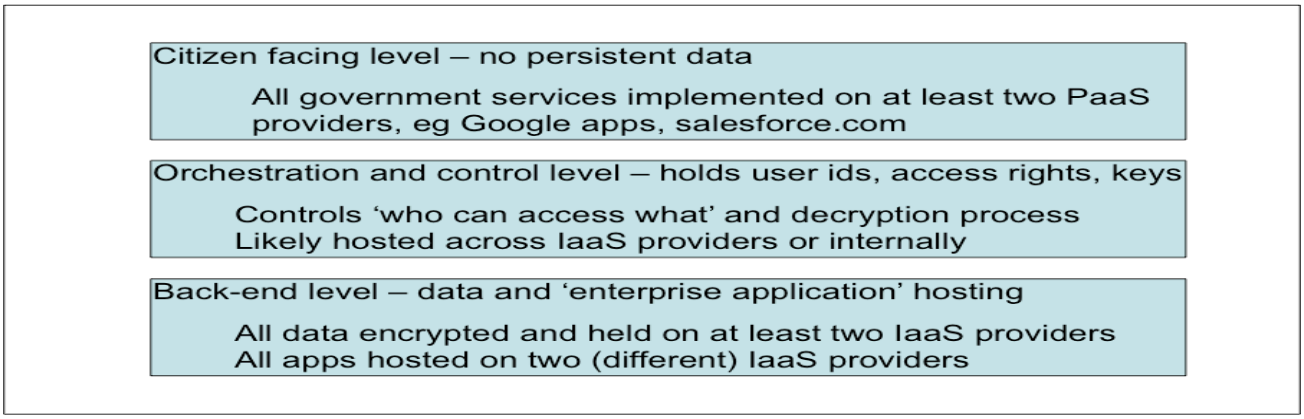


Figure 9: Model for using insecure Cloud computing services to underpin secure business processes

Successful implementation of the above model requires both selection of providers who can operate, and be compatible, at each level, as well as achieving integration between levels. The model is described below:

A "Front end" citizen facing services

At the citizen facing level, a choice of market leading "platform as a service" cloud providers (such as Google apps, salesforce.com. etc) can be used to configure presentational services (potentially in an agile manner) and then to present information-based services to citizens. There may also be a case for offering a basic in-house secure user portal. Risk is mitigated as only individual records are released to the front-end provider, once security checks have been

passed (and potentially only with the user's (ie data subject's)) permission.

B "Back-end" services

At the "back end" level, a combination of market leading "infrastructure as a service" cloud providers (such as Amazon Web services, RackSpace etc) could be used for (encrypted) storage of information, and hosting of "enterprise class" applications, which would be progressively replaced using a "services orientated architecture" model. Alternatively existing in-house databases can be used. Risk can be mitigated at this level by distributing data and services across multiple providers, in a manner where the loss or compromise of any single provider does not impact the confidentiality, integrity or availability of the overall business service.

C Intermediate Tier

At the "intermediate level" an "orchestration and control" layer will be needed, with operational policies proprietary to government. This layer will control encryption and decryption of data as and when needed, orchestration of transactions across "back-end" data stores and (internal or external) "platform as a service" providers, as well as user authentication etc. This (relatively small) layer needs to be highly secure as a compromise would potentially enable access to all data, services and users/customers. The cloud services brokerage may well choose to operate this layer on a reliable private cloud service, or on the clients' in-house systems.

D Summary – the three layer approach

It is essential to navigate a path between the extremes of risk; these range from being so averse to use of Cloud computing services that the journey to benefits realisation never starts, through to being over enthusiastic in adopting the services of major vendor's subsequently to find that "lock in" effects, security compromises, or services being discontinued, effectively means that excessive control of the service user's business has been handed over to the provider.

16.2.1.2 Hybrid cloud process design (A2)

The creation of the cloud services brokerages "go to market" strategy described in the section

above represents an investment the broker will need to make to enter the market. There are alternatives to the model identified above; for example working with security accredited cloud service providers.

Whatever the model selected, the cloud services brokerage will then want to offer a service to clients (A2) to provide specific business process designs, integrating the client's internal services with the broker's partner Cloud computing services.

16.2.1.3 Assurance services (A3)

An essential requirement of large organisations is to be able to demonstrate compliance with national laws, industry regulations and internal policies. Such compliance is demonstrated through independent audit; the assurance service to be provided by the cloud services brokerage is effectively the "readiness for audit". This will comprise both ensuring that service design and operational policies are auditable, and that the client can be confident that the necessary information will be collected and made available to the auditors so that compliance can be successfully demonstrated [63].

16.2.2 Buyer confidence

The Cloud Computing business model reduces barriers to entry for ICT suppliers, and is thus leading to growth in the number of ICT suppliers, as well as the availability of a broader and more diverse range of services. This thus creates a challenge for potential buyers of Cloud computing services; how to understand what is available on the market, to validate whether services meet (and will continue to meet) business needs, and to build sufficient confidence in suppliers. With hundreds of service providers the challenge of conducting a rigorous market assessment is daunting. There is thus scope for cloud services brokerages to provide cloud provider management services, as described below.

16.2.2.1 Manage provider relationships (B1)

For organisational buyers to recommend the selection and deployment of Cloud computing services, they will need to be confident that they understand what they are buying, that they have the means to scan the market and select the services that offer the best price/service

characteristics trade-off in relation to the business need, that relationships with providers can be managed effectively and that there is rapid substitutability with alternative services in the event of underperformance,

16.2.2.2 Contractual assurance (B2)

Challenges continue once Cloud computing services have been selected; organisations may find it challenging to manage a services portfolio with many tens of suppliers who all work to different contractual procedures, billing cycles and SLAs.

Given the proliferation of Cloud Computing services, trusted cloud service brokerage services can add value in identifying and validating cloud services suitable for use by a particular organisation or business community. Such an approach can share overheads, and reducing the costs of assurance, of managing the relationships with cloud suppliers, and of providing integration and support services (eg help-desk, transaction management). A central capability can also help expedite deployments when there are new business solution needs to be addressed.

16.2.2.3 Assure transparency/substitutability (B3)

Given that there is not agreement on a standard means of defining Cloud computing services, there is added expertise that can be provided in ensuring that all relevant dimensions of the service are considered when making a selection on behalf of the client. Where a deployed service ceases to be the best choice a substitution can then be proposed. Over time cloud services brokerages are likely to introduce automated capabilities to support this process.

16.2.2.4 Ensure delivery to end users (B4)

As described in earlier sections, it will be essential that business services incorporating Cloud computing services are properly supported. The services that a cloud services broker can provide could be based on a recognised service management standard such as ITIL 3, and include running a helpdesk, identifying which service is at fault when problems are reported, as well as tracking service performance over time, and obtaining service credits etc. The service management capability will need the ability to manage business services that comprise a hybrid

blend of in-house services provided on the client's legacy systems as well as both public and private Cloud computing services.

16.2.3 Establishing trust in the transition to the Cloud computing model.

Successful use of Cloud computing services requires a range of skills. Many organisations that are considering the use of cloud services recognise that they do not have all the necessary skills in-house; having a trusted partner they can work with to close any gaps that may arise will assist in boosting confidence to start the adoption process. Some of the specific services that cloud services brokerages may provide in this category are listed below.

16.2.3.1 Industry Association sponsorship to establish trust in the cloud services broker (C1)

It is clear that it will be critical for cloud services brokerages to establish their "trustworthiness". Reputation will help with this in time, but given the high dependence that organisations using cloud brokerages will have on these suppliers, it will be challenging for new entrants to convince user organisations that they really will be safe partners to collaborate with over the medium to long term.

Successful discharge of the activities listed in previous sections provides a context for trusted use of Cloud computing services, even in a context where trust in individual providers is low.

However, there is also the question of how to establish trust in the cloud services brokerage. This will not always be straightforward, particularly given that brokerages will be often smaller entities than the cloud providers they recommend, which may cause concern, eg are cloud providers' commissions influencing the broker's recommendations?

There are a number of options for establishing trust in brokerage services, including:

- Directly undertaking independent audits (which will be costly, and will reduce the overall benefits).
- Relying on professional accreditation through a trade body (e.g. the British Computer Society, the IEEE Computer Society).
- Encouraging sponsorship of brokerages by trade associations, encouraging brokerages to invest in understanding the requirements of a specific industry, and in selecting relevant

services, building know-how and tools for data standards etc. In such cases the trade association would retain audit rights.

Potentially, the trade association option brings several advantages:

- Selection of the recommended brokerages could be based on their potential contribution to enhancing the efficiency of their industry, as well as of individual participants.
- The brokerage, working with the trade association, could help establish and maintain data standards, and transactional interaction standards.
- Given the focus on a particular industry, the trade association would have an interest in managing risks, and would thus be likely to be proactive in exercising audit rights.

Risks could be further mitigated where a trade association selects two or three brokerages, and imposes some data and service transferability obligations on each. A goal would be that in the event of failure of one provider, member organisations could readily transfer data and services to others.

In conclusion, establishing trust may be accelerated through cloud services brokerages being commissioned by industry associations, who could then retain the right to transfer the business to an alternate broker, or introduce additional (competitive or complementary) brokerage services in light of experience.

The industry association sponsorship option potentially also brings the benefit of accelerated ability to realise cross industry efficiency and transformation initiatives. Cloud computing can enable legitimate sharing of information between business partners, for example between participants in the criminal justice system where cloud services brokerage could facilitate secure communication between the police, courts, probation and prisons, driving cross sector efficiency.

16.2.3.2 Regular independent audits of the cloud brokerage service (C2)

To evidence the legitimacy of trust, customers of a cloud brokerage service may wish to see evidence that regular audits of the brokerage are taking place. These could be commissioned by the trade association; or potentially by the brokerage directly from a recognised audit firm.

16.2.3.3 Coordinate service alignment (C3)

Ultimately, for organisations to be confident in deploying Cloud computing services as the standard approach to underpin their core business activities, there will need to be confidence that the use of Cloud computing services will result in more cost-effective outcomes, enhanced competitiveness, as well as mitigation of the risks of design, security, migration, management, supplier relationships and legal/other compliance.

Achieving this requires confidence in the ability to use combinations of Cloud computing services to achieve business requirements, as well as certainty that the internal capabilities are in place to use these services effectively.

16.2.4 Building capability in end-user organisations

There are a number of opportunities for cloud services brokerages offer services to assist in building the organisational capability amongst their clients to deploy Cloud computing services. Potentially these can include:

16.2.4.1 Efficient service selection (D1)

This would include providing education on the Cloud computing services available from the market that are relevant to the organisation's business needs. Guidance on using the tools provided by the brokerage to assist in selection would also be provided.

16.2.4.2 Integration and usage patterns (D2)

This service would be delivered in the context of the organisation's enterprise architecture. It would provide an approach for secure hybrid use of the organisation's information assets and services and the public and private Cloud computing services endorsed by the broker.

16.2.4.3 Cultural change and capability build (D3)

There is a considerable challenge to build the "soft skills" amongst ICT practitioners for there to

be a successful transition from conventional approaches to ICT to hybrid models. Education and development is needed at multiple levels, from the “big picture” of understanding how Cloud computing services can help the organisation, through to detailed training in a wide range of specific areas, for example how to assure end to end performance across multiple service providers.

16.2.4.4 Data migration and replication (D4)

Transferring data reliably and securely between systems and infrastructures can often be one of the greatest challenges in deploying a new system. There is scope for cloud services brokerages to build advanced toolsets to assist with migration, as well as a capability (that could be deployed either by the brokerage or by the client “on premise”) to maintain an up-to-date copy of data should there be a future decision to transfer the service to a new provider or indeed to bring it back in house.

16.2.4.5 Governance and risk management (D5)

Support will also be needed to assist organisations to update their internal ICT processes to account for the changed governance and risk management requirements when using Cloud computing services.

16.2.5 Initiation

Building on the range of capabilities described in sections, cloud services brokerages can also offer services to assist clients in determining their roadmap for cloud adoption. The services involved are described below:

16.2.5.1 Business readiness assessment and roadmap (E1)

The full transition to deploy cloud services in large organisations is likely to take place over a period of around a decade. Understanding the desired “end-state”, and the steps in getting there requires analysis that takes into account the organisation’s business objectives, the current state of its internal ICT, its customers priorities and expectations, and the range of relevant cloud services that is available.

16.2.5.2 Early proof of benefits (E2)

One of the outcomes from the readiness assessment will be identification of areas where it is relatively straightforward for cloud services to quickly bring significant benefits, and where the implicit challenges are readily easy to overcome. A successful "proof of concept" project will often be a precondition for an organisation signing up to a proposed cloud services transition roadmap.

16.2.5.3 Services orientated architecture roadmap (E3)

In addition to being confident that Cloud computing services can be used in specific contexts, organisations will also want to be confident that they are managing "the big picture" of strategic deployment.

For implementation of more complex business services, cloud services brokerages are likely to adopt the principles of Service Orientated Architecture, i.e. selecting reusable services (containing independent business or administrative logic) for a particular market sector or business community that can:

- comply with a standardised service contract.
- be loosely coupled, enabling service contracts to be abstracted from the underlying technical detail.
- be autonomous, stateless, discoverable, and composable into multiple configurations.

Such services could include user authentication, payments, mobile device integration etc.

The services that cloud services brokerages can potentially provide include:

- Overall assessment of an organisation's information assets and information services needs, to advise on the approach and priorities for moving to use Cloud computing.
- Providing guidance on the transition to using Services Oriented Architecture approaches, identifying the services needed and their relative priorities, as well as recommending the most appropriate organisational entity to lead the development of each.
- Design of an overall governance approach and model to ensure that a prioritised, strategic transition to Cloud computing services takes place, providing confidence that

there will not be unhelpful proliferation in the use of services and fragmentation of organisational data, and which mitigates the other "service specific" risks identified above.

- Linked to the above is another dimension of leadership development; specifically education and support of senior leadership in identifying how the flexible use of a broad range of Cloud computing services can "push the envelope" of the organisation's business model, enhancing overall competitiveness.

16.2.5.4 Business transformation opportunity (E4)

As organisations build experience with Cloud computing services, particularly if they are working with a broker who has expertise at the industry level, it is likely that support can be provided for developing the future strategy of the business. For example questions such as "are there better ways of doing business with partners?", and "are there improved ways of reaching our customers?" will need to be addressed. The cloud services brokerage will acquire expertise from across a range of clients, and will be well placed to provide advice in such areas.

16.2.6 Ability of cloud services brokerages to address obstacles identified from attempted Cloud computing deployments to date

The table below (is based on Table 14 and) has been annotated to show how the proposed services described so far in this chapter can potentially help resolve the issues that from experience to date, have been found to inhibit deployment of Cloud computing based approaches.

Issue	Net score	Addressed by service
Lock-in, with an imperfect supply marketplace inhibiting substitutability and thus price competition	-45	A1
Information security risk; inability to assure confidentiality, integrity and availability of services	-35	A2, A3

Difficult to provide assurance that services meet their full specification	-30	B1, B3
Lack of transparency of service design, security and management procedures	-25	A1,A2, B1
Unacceptable levels of risk are created by migrating existing “business critical” services from legacy to Cloud computing services	-20	A3, B3, B4
The cost of migrating data to Cloud computing services while preserving data recovery ability proves prohibitive	-20	D4
Corporate governance frameworks are unable to drive shift to use of Cloud computing, or to ensure successful use of services and realisation of benefits	-20	D5
The overheads involved in selecting Cloud computing services proved prohibitive	-20	B1, D1
Some combination of the issues listed undermines trust in business services that include a Cloud computing component	-20	D5, C2, C3
Legal concerns over ability to assure compliance with rules on privacy, data residency etc	-15	A3
Internal organisations lack the skills/culture for successful use of Cloud computing services, and are unable to build these	-15	D1, D2, D3, D4, D5
Transition to Cloud computing services is inhibited by high costs/lack of skills needed for designing, securing, migrating data to and managing Cloud computing services, or by legal/contractual constraints	-10	E1, E2, E3, E4
Relationship imbalance; suppliers may be too big (or too small) to take individual customers needs/concerns into account	-5	B1, B3

Table 17: Brokerage services to address obstacles to Cloud computing deployment

16.3 Operational processes for cloud services brokers

To efficiently and systematically deploy Cloud computing services, brokerages will need highly efficient processes, automated where possible. For example, how might a cloud services broker select its portfolio of cloud service providers?

Garg, Versteeg and Buyya proposed in their paper "a framework for ranking of Cloud computing services" [49] the establishment of a "service measurement index" (SMICloud) that offers comparative evaluation of cloud services based on user requirements. The proposal is that standard metrics are defined, categorised, grouped, and then used to calculate measurement indices that can then be used by customers to compare different cloud services.

The proposal builds on work done by the cloud service measurement index consortium that proposed the metrics are combined in the form of a service management index (SMI).

SMICloud proposes groups of metrics in the following areas:

- accountability, measuring cloud provider service characteristics as an important foundation of building trust, taking into account auditability, compliance, data ownership, provider ethicality, sustainability etc.
- agility, covering elasticity, portability, adaptability and flexibility.
- cost, expressed in characteristics relevant to the user organisation.
- performance, covering functionality, service response time and accuracy.
- assurance, the likelihood of a cloud service performing as expected or promised in the SLA, assessing reliability, resilience, service stability and engineering capacity.
- security and privacy, covering multiple attributes such as protecting confidentiality and privacy, data integrity and availability.
- usability, recognising the importance of the cloud service being easy to use and learn, which in turn depends on multiple factors such as accessibility, ease of deployment, learning ability and operability.

It is clear from the proposed SMICloud framework that developing a full understanding of each specific cloud service is a complex task in its own right; if done manually developing such

detailed understanding of the many thousands of services that exist, and which are continually changing and evolving, will be beyond the scope of any one organisation.

The SMICloud framework is helpful in that it makes clear that objective assessment and comparison of cloud services needs to take into account a great many factors. The implication is that if a manually orientated unstructured approach is adopted, this is likely to result in limited coverage, high assessment costs and inconsistent outcomes.

Additionally, for the foreseeable future there will be some characteristics that cannot be expressed in metrics; for example a service's ability to cope with say a specific piece of business logic underpinning an particular insurance company's underwriting process will for the foreseeable future require human evaluation.

Hence while through comparison of metrics a cloud services broker may be able to derive a service shortlist, other than where services are totally commoditised and operating to an identical specification, it is unlikely to be practical to completely automate the optimum selection process -- at least for the next five years.

16.4 Chapter conclusion -- There is a market opportunity for cloud services brokerages; establishing trust is critical, and organisations that invest in building automated capabilities will gain competitive edge.

Cloud computing has the potential to reduce some elements of ICT costs by 65% to 85%. This level of cost reduction opportunity justifies a deliberate strategy to ensure the benefits of Cloud computing are realised.

Yet achieving secure deployment of Cloud computing for complex line of business processes is not straightforward; while some types of Cloud computing deployments are relatively achievable, such cases account for only a relatively small minority of today's ICT budgets. Achieving the breakthrough into mainstream will come with the use of Cloud computing services for core business processes. However many organisations lack the knowledge of cloud service providers and/or the skills to achieve this increase. The adoption of cloud brokerage services by large organisations and business communities is recommended as part of the strategy for moving forwards.

Cloud services brokerage capability can be built in-house (requiring investment in people, methodologies, skills development and relationship management with cloud services vendors), or can alternatively be bought in from a specialist provider. Such cloud services brokerage providers will need to be independent of cloud computing service providers, and may originate from “pure play” start-ups, or from established “vendor neutral” firms such as IT distributors.

The author’s opinion is that large organisations will adopt a hybrid approach, developing a certain level of capability internally, and selecting a range of cloud services brokerage partners to use in more complex cases. For example at the National Offender Management Service, deployment of the Huddle collaboration service was done using in-house resource, whereas a cloud services broker was used to migrate the Offender Interventions Database from an in house Microsoft Dynamics CRM implementation to the Microsoft 365 CRM public cloud service. The cloud services “broker” in this case provided assistance with configuration, data migration, report writing and initial user support.

Cloud services brokerages need to be trusted (and trustworthy) to consistently act in the long-term interest of the users of Cloud computing services. They need to have the credibility to deal authoritatively with cloud services vendors, and thus need to be of reasonable scale in their own right. In addition to selecting, integrating and configuring cloud services, there is also scope for cloud services brokerages to add value by creating community services and coordinating community data standards. Trade associations may thus be well placed to commission cloud services brokerages, analogous to the banking industry’s sponsorship of independent ‘shared services’ organisations including Visa, MasterCard, VocaLink (BACS and Link) etc.

Given the scale and diversity of many large organisations, the recommended approach is to adopt the "business communities" approach recommended by the G Cloud phase 2 programme team, with trade associations appointing one (or more) cloud services broker(s) for each community. Cloud services brokerages working on behalf of government will need to operate in a federated structure so that where a service is required by multiple communities, demand is aggregated, and the overhead of validating relevant services is incurred only once across government.

There is likely to be significant growth in the Cloud Services Brokerage segment over the next few years, and initially at least, growth is likely to be self-reinforcing, as the greater the range of services and expertise possessed by cloud services brokers, the more compelling will be the

benefits they can offer in reusing their skills and services portfolio to drive yet lower transition costs for subsequent customers, thus delivering ever improving business outcomes.

Further work is needed in to define the services to be provided by cloud services brokerages, to initiate their development, and to encourage the creation of automated services. Over time the unit cost of cloud services will continue to reduce and, as scale and maturity becomes better established, the cost of providing cloud brokerage services will reduce as maturity, scale, automation, standards and reuse and similar effects provide growing benefits.

Part 5: Key findings and further research areas

This final part of the thesis summarises the conclusions reached and the recommendations for further work.

Many large organisations, including UK government are making progress with the deployment of Cloud computing services, both public and private, with the initial focus often being on relatively self-contained deployments. The first 18 months of the UK government CloudStore has built useful experience on demand and usage. There is considerable further potential both to extend deployments into core line of business processes, and to organisations that have not yet commenced deployment. However, many large organisations lack the knowledge of cloud service providers and/or the skills to achieve this increase. Adopting cloud brokerage services is recommended as the strategy moving forwards.

Given the scale and diversity of many large organisations including governments, the recommended approach is to adopt the "business communities" approach proposed as part of G Cloud Phase 2, appointing a cloud services broker for each community. These brokers though will ideally to be sponsored by a body that represents users and that can enforce audit rights where needed. They will need to operate in a federated structure so that where a service is required by multiple communities, demand is aggregated, and the overheads of validating services are incurred only once across government.

Further work is recommended to in a range of areas, including standards, soft issues and technical architecture. Recommendations for further work are set out in section 18.

17.0 Conclusions and recommendations for further work

The main conclusions from the research conducted between 2009 and 2013 are summarised below:

17.1 Cloud computing is by no means a new concept

The concept of utility computing is over 50 years old, and is relatively well established for some community services, for example air ticket booking, ATM sharing etc

The “client/server” era of the 1980s to 2000s led to a proliferation of servers and data centres, moving the industry away from the benefits of utility computing. Addressing each new business problem tended to result in a new ICT solution, requiring new servers with a unique software configuration, leading to proliferation of large numbers of systems with low utilization levels. Over time the inefficiency of the approach became progressively more apparent. Starting from the late 1990s, organisations such as salesforce.com began to show that “multitenanted” services could yield higher levels of efficiency and lower unit costs.

17.2 But the size and scale of Cloud computing providers, and the level of cost reductions achieved, means the delivery model is a “game changer”

The trend towards Cloud computing accelerated with the advent of very large consumer Internet firms, such as Google and Amazon. These organisations required both massive computing capacity and very high levels of flexibility, as they needed to ensure their computer capacity could be readily redeployed onto the next business application given the rapid rate of change prevalent in the industry. These organisations decided to adopt a standard for “virtual machines” that could be used by all applications, and which could be underpinned by a range of hardware systems; enabling the latest processors and systems to be used for capacity augmentation.

Having large pools of standardized virtualised machines in place brought other advantages too; firstly it became practical to build data centres to a larger scale and manage them more efficiently with relatively small teams of people. Secondly the degree of automation in the data centre increased substantially; this brought both cost reductions and reliability improvements (by

eliminating much of the scope for human error; which is traditionally one of the top causes of data centre service issues). The automated data centre management systems created the possibility of computing capacity being marketed under the "Cloud computing" concept; with the addition of e-commerce front ends and automated management services it became possible for users to purchase ICT capacity on the Internet, and for this to be provisioned in (near) real-time. As firms such as Amazon and Google realised that the capabilities they had built for their core business positioned them to enter this potentially lucrative new market, the Cloud computing era accelerated.

The Cloud computing concept quickly found favour with a number of constituencies; including business users frustrated by corporate ICT's long lead times, by environmental campaigners who recognise Cloud computing as being more compliant with the "green" agenda, and by business leaders who are driven to reduce costs during a period of austerity. Some of the examples of early successful usage helped to build momentum, for example Japan Post's large-scale deployment of salesforce.com to provide new front office systems. By 2008 there was widespread interest in the phenomenon, and awareness of the potential for Cloud computing, over time, to become the dominant approach to delivering enterprise ICT.

The potential benefits of Cloud computing are multi dimensional; cost reductions are often the initial focus but can be over emphasised; other benefits include agility, enhanced collaboration and accelerated innovation.

Cloud computing services are provided on a "as a service" commercial basis and are generally regarded as falling into three main categories covering:

- infrastructure; processing, storage and communications.
- platform; tools to assist with development of business applications.
- software; "ready to use" business services for specific tasks such as customer relationship management or e-mail.

Deployment of Cloud computing can be on a private, public, community, managed or hybrid basis. However, there is complexity in using the services, and trust is required in the providers. The combination of these factors, coupled with lack of detailed control over how the cloud provider designs and manages its systems means that there are significant risks in using Cloud computing services. Managing these risks effectively, while still preserving the benefits of the Cloud computing approach represents a challenge. For example if a cloud provider ceases to

meet expectations how practical is it to get an organisation's data from the cloud provider, in a format that can be reused internally or by another service provider?

17.3 Continued deployment of Cloud computing services seems inevitable

Cloud computing has clear potential to reduce ICT costs and enable improved delivery of information and transaction services to businesses. The scale of the cost savings that are achievable at the datacentre and application levels (65% to 85%) provides sufficient incentive for progressive and sustained replacement of conventional ICT with cloud-based services, even though overcoming the barriers that apply particularly to complex deployments will take a number of years.

Chapter one (Introduction) identified the central questions to be addressed in the thesis as:

- Firstly whether large organisations, particularly public sector or governmental, can realise benefits by transitioning from the ICT delivery models prevalent in the late 2000s to use Cloud computing services?, and
- Secondly, in what circumstances can the benefits best be realised, and how and when can the associated risk reward trade-off be managed effectively?, and
- Thirdly, what steps can be taken to ensure maximum benefit is gained from using Cloud computing? This includes a consideration of the obstacles, both technical and organisational, that need to be overcome to realise these benefits in large organisations.

There is no doubt that Cloud computing offers very substantial benefits, and that these extend well beyond cost reduction to better enablement of business innovation. Cloud computing services can provide rich functionality, beyond that which an individual or organisation could justify developing internally. In an age characterised by ICT-based innovation and consumer choice, use of Cloud computing services brings the possibility of meeting users expectations for services such as mobile access, integrated social networking, or access to mapping and location services which an organisation might otherwise be unable to afford as an internal development project. It seems likely that consumer expectations will provide a strong incentive for enterprises to make growing use of Cloud computing services.

The above provides an example of how use of Cloud computing can potentially enable organisations to accelerate innovation; this applies in other fields too. For example Wilcox et al (section 5.3) contend that Cloud computing will result in organisations transitioning from

products to business services, placing greater emphasis on service performance, and enabling reconfiguration of supply industries. Wilcox's paper argues that ICT will also see a transformation in industry structure to a relatively small number of providers of utility services, a large group of specialist providers with distinctive industry expertise, and an elite group of service integrators who will partner with enterprises for provisioning of the services ecosystem. This resonates with the work of the Nobel laureate economist Ronald Coase [42] who in 1937 hypothesized that firms exist on the basis they are able to reduce internal transaction costs i.e. the costs of finding a supplier, the cost of transacting, and subsequent costs of coordinating delivery. Cloud computing has the potential to impact transaction costs in many industries, including the ICT industry itself, and thus to act as a change driver for organisation and industry structures.

Hence there is some justification to the claims made by Cloud computing providers that their services can help reduce costs, improve service and enable faster and more effective innovation.

However, there are significant barriers, challenges and pitfalls to overcome:

- Compared to other professions, ICT is relatively immature in its methodologies and has not been able to consistently reuse existing assets. This has resulted in a chronically high level of "reinventing the wheel".
- Enterprise architecture and governance initiatives to achieve reuse have been slow to gain traction.

The overall conclusions are:

- some cloud services can already be used within organisations on a "stand-alone" basis, with relatively small overheads and readily attainable benefits.
- however the straightforward deployments represent only a minority of ICT spend.
- using cloud services for the organisational specific "line of business" processes where much "unique business value add" is generated is much more challenging.
- addressing the majority of more complex ICT requirements using Cloud computing services requires new skills, that are generically described as "cloud services brokerage". Today (2013) such skills are difficult, complex and time-consuming to build internally, and potentially hard to source externally.

17.4 Cloud computing has potential to bring substantial benefits to large-scale enterprises through economies of scale/lower unit costs.

However, there are also significant risks and costs in moving to widespread deployment of Cloud computing services, with analysts concluding that by end 2012, Cloud computing services had captured only 5% of corporate ICT budgets.

The starting point for using Cloud computing services in most organisations will generally be for relatively simple services; these may include the use of in-house “private clouds”, supplemented by the use of public cloud services for non business critical activities where risks can be managed; for example development and test services, or collaboration with other organisations. These “use cases” however only account for a relatively small proportion of ICT spend.

Potentially much larger benefits can be obtained if cloud services can be applied to automate core high-volume business processes. Doing so however will typically require the use of a mix of in-house services (e.g. authentication services, access to data), and the use of a range of external services integrated with case management, with business rules applied to determine the next step in the transaction.

One of the key characteristics of transactions is that if they do not complete in full then all the steps need to be “unwound”, and the orchestration process that combines the use of in-house and cloud services will need to accommodate this essential requirement.

“Soft issues” represent a major barrier, for example most organisations lack the capability and in-depth knowledge base needed to move with confidence to use cloud services for core business processes. There are also significant concerns over security, including unintentional breach of legislation.

17.5 UK Government is committed to a hybrid cloud ‘cloud first’ strategy

The UK Government published its Cloud computing strategy in autumn 2011; this positions the G Cloud as a hybrid cloud consisting of public, private and potentially community cloud services.

It is recognized that changing the way government buys ICT is fundamental to achieving the desired benefits.

There is also recognition of the scope for using cloud services to deliver to a wide range of devices, including mobile Internet.

The published strategy reasserts the principles of Cloud computing and announces a "public cloud first" policy. It sets out the anticipated benefits of cost reduction and increased flexibility, acknowledges the deployment models of public, private, hybrid and community clouds, sets out the concept of G Cloud being an ongoing programme of work, rather than a single entity, and acknowledges the need for behavioural change and development of the market.

However, compared to the G Cloud definitional work that was done in 2009/10, the published strategy includes some changes in emphasis; more use of public cloud and less emphasis on establishing private and community cloud services, positioning the CloudStore as an online catalogue without the proposed provisioning and service management tools, more emphasis on SMEs in line with government policy, more emphasis on the use of purchasing frameworks, less emphasis on addressing complex line of business applications or on mandating the transition of existing services. There is also a simplified initial approach to ICT Service Management and Information Assurance; this reduces the work needed at "the centre", but places more emphasis on assurance by end-user organisations.

Three main areas of risk are identified; the potential for lack of aligned leadership, the challenge of building internal ICT capability to deliver in the new environment, and the potential for an unsatisfactory response from the ICT supplier marketplace.

17.6 Initial deployments will focus on relatively straightforward cases, however these will not have a major impact on the core of ICT activities

Initial business deployments tend to be concentrated in areas requiring relatively self-contained business solutions, where there is no suitable existing ICT solution, and where data is not highly sensitive. The services supported have thus been those such as web hosting, e-mail, office software, collaboration software and storage as a service.

In summary, while momentum for "simple deployments" continues to build, the percentage of ICT spend such deployments can address is relatively limited. Further work is needed to determine the approach for line of business applications to accelerate progress.

17.7 Using commodity Cloud computing services for complex organisation specific "line of business activities" is difficult and challenging

For individual organisations using ICT, the risks and complexity of using combinations of Cloud computing services to replicate business critical processes poses a substantial challenge. While the allure of future cost savings and potentially better services is attractive, particularly on a project by project basis the overheads of "making it happen" will often be prohibitive. Few organisations will initially want to make the upfront investment needed to establish an effective internal capability to successfully use Cloud computing services.

Specifically if a user organisation has to scan the market to assess many thousands of competing providers, and then do a detailed assessment of shortlisted services on criteria such as functional fit, non-functional requirements, data standards, disaster recovery, peak load performance, data location etc the costs will be substantial. Furthermore potentially much of this work will have to be (perhaps almost continually) reassessed; as Cloud computing providers routinely update their services. The challenge becomes even more complex where a business need is addressed using two or more Cloud computing services, where the interactions also need to be taken into account.

17.8 Other barriers need to be addressed to accelerate benefits realisation from Cloud computing;- many of these relate to leadership, culture, capabilities and processes

Surveys have confirmed that despite government organisations perceiving benefits such as flexibility, agility, lower costs and improved service levels from using cloud services, perceived risks are slowing take-up. The top concerns that delay adoption of Cloud computing services are security concerns, perceived risks from using "unproven" technology, lack of confidence/control of data residency, and lack of a framework for building the business case.

There are also some significant human barriers; for many practitioners (CIOs and their teams) Cloud computing changes, and thus potentially threatens established roles. Specifically some perceive that CIOs risk losing relevance and being bypassed, and CIOs therefore need to

demonstrate a greater contribution to business strategy and information management, and to demonstrate how ICT can add value in the selection and use of cloud services. Achieving this however requires not just a change for the CIO and their senior team, but rather a change in culture across the ICT organisation.

There is also the need for processes and methodologies on how to use cloud services to address business needs, and to mitigate what many currently see as exceptionally high levels of security, commercial and business risk.

Interestingly, technical issues are seen to present less of a barrier than people and process issues; technical concerns include the ability of the network to deliver, how to ensure applications design meets non-functional requirements in the cloud environment, and the desire to make faster progress on setting standards.

In summary, today take-up of Cloud computing services is being impeded by a range of issues including security concerns, lack of clarity on legal issues, networking risks, lack of mature design and service management models, lack of governance frameworks that are relevant to Cloud computing deployment, and lack of standards and in-house capability.

17.9 There is a market opportunity for cloud service brokerages; organisations that invest in building automated capabilities will gain competitive edge.

This thesis has set out the very significant benefits that can be attained from Cloud computing, and how adoption is underway starting largely with relatively straightforward business requirements where commodity cloud services meet the need on an “as is” basis.

It is clear though that the benefits can extend much further, right through to replacing the majority of currently deployed ICT that has been designed and/or configured to deliver the unique needs of specific organisations.

There are however significant barriers to overcome, and given the global nature of cloud providers, their very large-scale, and the focus of many on the consumer markets many organisations will not wish to become over dependent on their services. Nevertheless, these services offer attractive benefits, including business agility and cost reduction.

As set out earlier the obstacles that need to be overcome include:

- Demonstrating compliance with legal and security requirements (greatest challenge).
- Establishing confidence amongst Cloud computing buyers that relationships can be managed, that services can be assured and that suppliers will not exploit their power in the future.
- Establishing trust amongst users of Cloud computing services.
- Building buyer capability to select services, manage transition, migrate data and manage service providers.
- Initiating Cloud computing based projects (less challenging).

The SMI cloud research provides an example of how a tool can be used to automate one of the roles of a cloud services broker, namely the selection of services. It will be possible to create similar approaches in many other areas.

17.10 Significant investment is needed in cloud service brokerages to drive the potential of Cloud computing

Systematic deployment of Cloud computing services in complex contexts requires toolsets to reduce upfront costs, so that it is more cost-effective to use Cloud computing services on a project-by-project basis. It is this that creates the opportunity for cloud services brokerages, and for these types of organisation to offer a range of services across a life cycle as depicted below:

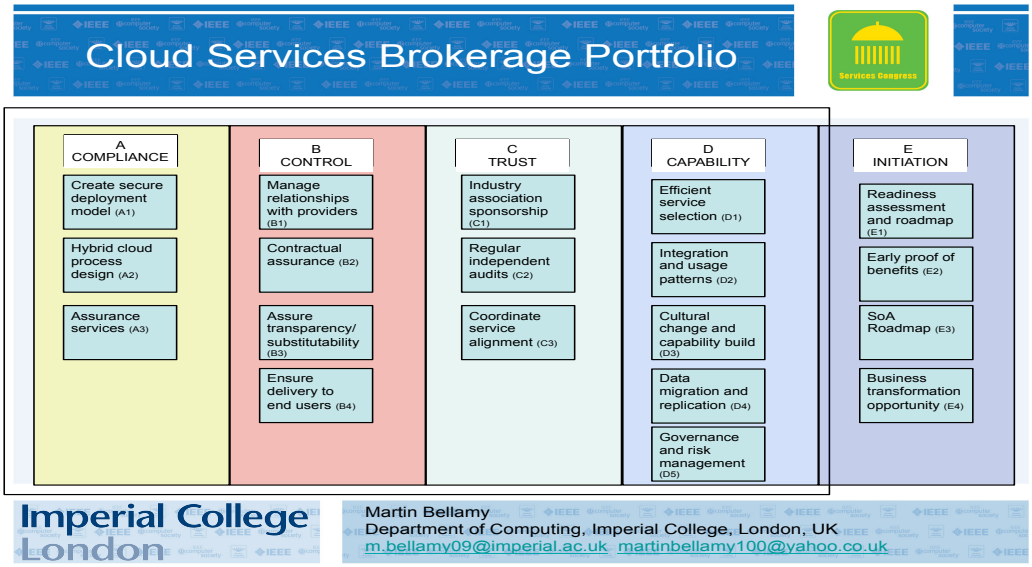


Figure 8: Cloud Services Brokerages – Potential Services

While there will be significant investment required to provide the range of services indicated above, the opportunity to leverage savings of up to 65% to 85% on ICT "run and maintain" costs makes pursuit of this highly attractive. When considering the significant amount of effort required to address the above issues, it is evident that undertaking these activities on a project by project basis will incur prohibitive costs other than in the most simple of cases. Engaging such a broker brings the potential to realise the benefits of Cloud computing services, including those designed for the very large-scale consumer markets, while being able to mitigate the inherent risks.

The G Cloud Phase 2 programme team specified the key roles for what amounts to an insourced Cloud Services Broker. Under the working title of the "G Cloud Authority", the intention was that the brokerage service would aggregate demand from across public sector organisations, source cloud services that meet agreed technical, commercial and security requirements, provide the necessary integration and service management capabilities, and catalyse the shift from existing ICT delivery models to the use of Cloud computing.

The services to be provided by the G Cloud Authority covered aggregation and standard setting, integration and customisation. It would be an intermediary between public sector organisations and cloud services providers.

Cloud service brokerages need to be trusted (and trustworthy) to consistently act in the long-term interest of the users of Cloud computing services. They need to have the credibility to deal authoritatively with cloud services vendors, and thus need to be of reasonable scale in their own right. In addition to selecting, integrating and configuring cloud services, there is also scope for cloud service brokerages to add value by creating community services and coordinating community data standards. Trade associations may thus be well placed to commission cloud service brokerages, analogous to the banking industry's sponsorship of independent 'shared services' organisations including Visa, MasterCard, VocaLink (BACS and Link) etc,

There is likely to be significant growth in the Cloud Services Brokerage segment over the next few years, and initially at least, growth is likely to be self-reinforcing, as the greater the range of services and expertise possessed by cloud services brokers, the more compelling will be the benefits they can offer in reusing their skills and services portfolio to drive yet lower transition costs for subsequent customers, thus delivering ever improving business outcomes. UK government is not planning to set up an internal Cloud service brokerage, and this therefore represents an opportunity for the market.

A business case was produced as part of G Cloud Phase 2, in cooperation with the supplier community that indicated that, once fully implemented, a transition to Cloud computing brings the potential to reduce public sector ICT costs by between 15% and 25%. Subsequent analysis has identified scope for savings of up to 45%. Additionally citizen facing business processes could be re-engineered to address the "digital by default" public service delivery agenda, accelerating the ability to implement new strategies and policies.

17.11 Automation of the services to be provided by cloud services brokers will yield further benefits; however the standards to do this in full are not yet available

Ideally, organisations would be able to select trusted Cloud computing services from a "CloudStore" online catalogue. Following purchase, the service would be automatically instantiated and integrated with the organisations' role-based access control system; this in turn would provision the new service with the organisational data needed to meet the end-user's requirement. Simultaneously, the "behind-the-scenes" integration needed to manage and secure the service would automatically take place; i.e. with links to monitoring and helpdesk services, security, intrusion detection, monitoring and audit etc.

However, from a technical architecture perspective, the standards needed to automate the above process do not in the main exist. While much can be done on a relatively manual basis, this comes at a comparatively high cost. While such capabilities are likely to develop in time, this requires both development of the "cloud services broker marketplace" to provide these types of services, and over time, agreement on industry and proprietary standards so that such provisioning can be automated.

Another desirable benefit from the technical architecture is resource pooling. One of the core "value adds "of Cloud computing is that resources can be shared across multiple users. The economic model however depends on not all users requiring simultaneous "peak load" access. Inevitably such conditions will rise, albeit rarely. To mitigate the risk of service degradation during such periods the concept of "cloud busting" has been widely discussed. This involves additional capacity being sought from another provider at peak periods. While proprietary standards for achieving this exist; for example between VMware customers, there is not today a widely adopted open industry-standard for achieving the same effect. Such a standard would allow cloud service brokers to offer "burst "services, creating an additional revenue stream, and

helping to mitigate service risk. Such standards would need to cover technical capacity (compute, storage, communications), request period (large-scale network capacity will be needed to provision such services sufficiently quickly) as well as guarantees of non-functional requirements including security, data residency, and other attributes.

While the full vision will take many years to realise, there is much that can be done now. Today, a number of organisations have successfully implemented internal private cloud models, typically in conjunction with a data centre rationalisation programme, and have reported cost reductions in the region of 30% to 60%. Bechtel is an example. Organisations are also making widespread use of public cloud services for specific applications; for example Japan Post is using salesforce.com to provide front-office services to 100,000 users. Likewise General Motors is using Google apps to provide e-mail and office software to the majority of employees.

17.12 A 'defence in depth' strategy is needed to manage Information Assurance challenges when using Cloud computing services

The transition to Cloud computing services brings upside and downside risks from the Information Assurance perspective. The downside risks include there being less, if any, control over changes made by the Cloud computing provider. Additionally the concept of using virtualisation technology to support multiple organisations and their information on the same physical device is relatively new, and there may be still security vulnerabilities that have not yet been discovered. There is also the reality that some Cloud computing providers prioritise features and early delivery to the market over and above exhaustive information security validation.

There are upsides too; - potentially fewer services will need to be assured and thus increased assurance effort can be expended on each.

While the core risk areas of loss of confidentiality, integrity and availability remain unchanged, the global nature of cloud service providers means there is less control over where data resides. With some Cloud computing services data can potentially travel outside national borders, and this may bring new risks such as personal vetted to different levels, potential interference by overseas governments and breach of legislation that may restrict where data can be moved to.

Given the proliferation of Cloud computing services the overhead of assuring many individually will be prohibitive, and the concept of centralized accreditation of cloud services has the potential to bring economies of scale as well as to increase business agility. However, this will not be a substitute for consideration of the specific usage context of the service, the inherent information and the needs of the user community. This work will need to be done on an organisation-by-organisation basis; this will also need to take account of the likelihood of sophisticated threat actors having sufficient interest in information to make a breach a serious possibility.

Governments in the US and UK have introduced new Information Assurance frameworks which are in part intended to remove some of the barriers to using Cloud computing services. These approaches recognise that good commercial encryption/security technology is now suitable for the majority of public sector data and services.

Amongst the areas to consider are user and employee access control, protective monitoring, forensic readiness (collection of digital evidence), clarity on roles and responsibilities, having a security incident management policy, organisational standards for data encryption, both “at rest “and “in-flight”, and a sanitisation policy to ensure that data is securely removed when use of cloud service ceases.

17.13 A strategic approach is needed for ICT service management when using Cloud computing services, with focus on how to ensure service continuity and on preserving data should a provider fail

Service management using Cloud computing services presents new challenges; as in other areas there is much reduced control over the providers approach. Further the commoditised “as is” nature of services means that it will often be necessary to use two or more together to achieve a particular business process outcome. Given the limited control of any particular customer, it will usually not be possible to understand the engineering detail of how the service has been constructed, and thus also impossible to model fully how the service will perform under various extreme scenarios. It will be necessary therefore to rely on commitments and assurances made by the Cloud computing vendor and (where available) those of auditors.

For the foreseeable future establishing trust in the Cloud computing suppliers will therefore be essential. In the longer term these risks may be partially mitigated should standards and market

transparency develop to the point where “instantaneous transfer” to an alternative service becomes possible.

In the near-term organisations will need to ensure that there is a framework for managing Cloud computing services, and that this encompasses agreed approaches for sourcing, governance, procurement and measurement.

Where a cloud service is being used together with internal services, or where several cloud services are being used together, there will be a need for a “service integrator” who will be accountable for achieving a predictable end to end business service outcome that builds on the SLAs of each cloud service provider.

Standards for Cloud computing ICT service management would be of benefit to service brokers in predicting, measuring and sustaining service delivery outcomes. Currently there is a lack of maturity in this area; while the IT infrastructure library (ITIL) provides a possible framework, it was specified with conventional ICT delivery in mind, and is currently somewhat inconsistently deployed to varying levels by organisations.

This implies therefore that consuming organisations will need to do significant work with each cloud provider before adopting services for high priority business processes.

The cost of doing so for individual organisations will be significant, and it may therefore be preferable to contract out this role to a third party organisation. Phase 2 of the G Cloud programme identified such a role for an “Integrated Services Manager”; this is one of the roles that could be performed by a cloud services broker.

Tooling will also be required; for example so that the helpdesk and the “service dashboard” can provide a holistic service that includes Cloud computing services.

As in other areas it is clear that there are there are complex challenges to address, and again a phased approach is inevitable; starting with relatively straightforward use of Cloud computing services in less business critical areas.

17.14 The marketplace for Cloud computing services is far from perfectly competitive, with providers deliberately and extensively differentiating services

From the buyer's perspective, there would ideally be a "perfectly competitive market" for Cloud computing services. However, while Cloud computing represents a step towards this ideal, there are significant shortfalls including lack of consistency of services, significant entry and exit barriers (costs), and high transaction costs for corporate customers.

The commercial barriers are lower where organisations' requirements are relatively homogenous, and can therefore be satisfied by a number of Cloud computing services on an "as is" basis. For example hosting websites, commoditised applications such as e-mail and basic word processing, and development and test services are well suited as starting points.

Developing a more competitive marketplace will require time, and could potentially be stimulated by the specification of standards that will apply across a large community group such as government. This will be enhanced if such standards can be aligned with those being specified, for example, by the EU or US governments.

From the commercial perspective objectives include ensuring changes are simple and easy to achieve, having transparent and comparable pricing, putting in place a standardised purchasing model, having confidence that suppliers will meet minimum technical, commercial and information assurance standards, and working within a common governance framework.

In common with the technical, service management and information assurance areas, from the commercial perspective a phased approach will again be needed, starting by building experience and confidence in use of relatively simple services in lower risk areas of business, building experience over time.

17.15 Organisations will need to accept, and effectively manage new types of risk, to succeed with the use of Cloud computing services

Deploying Cloud computing services, particularly for core business processes involves accepting and managing new types of risk. Given the ever-growing diversity of the marketplace, the cost to consumer organisations of building and maintaining an understanding of the entire breadth of

Cloud computing services available in the marketplace will be prohibitive, as will the overheads of integrating, operating and managing anything other than a very simple portfolio of services.

Organisations will need to consider their information risk appetite, and put into place processes to ensure that this is addressed through the selection and usage strategy of Cloud computing services. Given the lack of control over providers, organisations may wish to consider either appointing a broker responsible for mitigating security risks, or using combinations of cloud services in a way that mitigates the risk presented by any single provider, for example by encrypting data before transferring to the cloud provider, and ensuring that services can be sustained even where an individual cloud provider fails.

Achieving secure use of Cloud computing services for mission-critical processes requires investment in capability, service design, monitoring and management.

Many organisations lack the knowledge of cloud service providers and/or the skills to make broader use of cloud services. To acquire the necessary expertise, organisations should consider procuring assistance from cloud brokerage providers to support the development of a Cloud computing strategy, and to assist with the initial deployments of Cloud computing services that should initially be to address new business needs. This can subsequently extend to assessing where Cloud computing services can be used to replace existing “on premise” ICT systems.

Specifically in the case of governments, given their scale and diversity, a potentially attractive option for migrating to cloud services is to focus implementation on the "business communities" approach recommended by the G Cloud programme. This would involve appointing a Cloud Services Broker for each community. These brokers though will need to operate in a coordinated (eg federated) structure so that where a service is required by multiple communities, demand is aggregated, and the overheads of selecting and validating services are undertaken only once across government. For private sector organisations, cloud service brokerages could potentially be appointed for business communities by their trade associations.

NIST states that using Cloud computing services potentially exposes user organisations to new risks, in that Cloud computing systems are complex and can be of enormous scale. As a result failures can emerge from events that are difficult to predict, and where this occurs the consequences can be significant, with substantial time required to diagnose and repair faults. In

designing the technical approach for using cloud services organisations need to be conscious of these risks, which in part can be mitigated by using a range of cloud services, avoiding complete dependency on any single provider for a "business critical" service or data.

17.16 The UK public sector is gaining valuable experience from the growing success of CloudStore

The experience of the UK government CloudStore, and the 'cloud first' policy, has enabled the UK public sector to build valuable experience in the use of Cloud computing services.

The G Cloud is being established as the public sector "brand" for trusted Cloud computing. Services that have been accredited to be compliant with G Cloud standards are being made available to public sector organisations via an online catalogue, the CloudStore. This enables both simplified discovery of services that are suitable for use by public sector organisations, and aggregation of purchasing power to achieve the lowest possible unit price. Simultaneously CloudStore is for the first time making some ICT services available to public sector organisations on a "pay per user" basis, which in turn is accelerating innovation and cost reduction.

17.17 The "change journey" for deploying Cloud computing services will take place over a decade or more, and involves a multilevel transformation of the supplier and consumer marketplaces, affecting people, process and technology

Cloud computing is based on relatively mature technology, with the concept being founded on a refreshed commercial model, enabling the deployment of capabilities that allow systems (but not data) to be shared between multiple users.

It is also clear that for enterprises with significant security requirements, expectations have run ahead of reality. In 2009/10 the main focus of Cloud computing innovation was from the consumer focused providers who were in general pursuing delivery of "features" as a higher priority than "world class information security". A number of barriers have been identified, not least that exploiting Cloud computing services requires changes to the approach for managing ICT in the enterprise, in turn requiring some additional skills beyond the experience of many (perhaps most) current ICT practitioners. There are also commercial and legal barriers; including the lengthy duration of many ICT outsourcing contracts, and lack of clarity over issues such as whether the "global information architectures" of many cloud providers (meaning data can go

outside national borders) creates a prohibitive compliance risk.

It is clear therefore that the transition to using Cloud computing services will be a progressive process that will start with what is immediately practical and beneficial, and which needs to be regarded as a "journey" probably of a decade or more. During this period the ICT industry will provide an ever growing range of more suitable services, and user organisations will need to build and develop the skills needed to successfully deploy and manage Cloud computing providers. Over time, cloud service brokerages will emerge to offer a growing range of services to help organisations with this task. Progress can be expected to accelerate over time as the range of cloud services providers, and the numbers and capabilities of cloud services brokers, together enable progressively more compelling "buy propositions" to be put to user organisations.

17.18 The broadly based volunteer approach to this research has yielded input from a wide variety of perspectives; -this approach should be considered in similar cases moving forwards.

The formation of the multi-organisation, volunteer-based G Cloud programme team, and its eight work strands structure, proved a highly effective research model that developed some leading edge thinking that resonates with that of academics and industry analysts

18.0 Recommendations for further work

There is scope for further work in the areas of organisation, governance, capability building and cultural change, supplier management, application design, solution design, service management models, technical standards, information assurance, cloud service brokerages and the techniques for developing business cases for Cloud computing deployments.

The priority areas include the research areas listed below:

18.1 To consider the organisational models and governance structures that will accelerate realisation of the benefits of Cloud computing

Use of Cloud computing services requires that user organisations can have confidence that their business requirements will be met, and will continue to be met in the future. This needs to include future requirements that cannot currently be fully specified. Achieving this requires confidence that necessary business enhancements can be achieved through using combinations of services.

18.2 To identify how best to ensure information assurance for organisations making use of cloud services

This requires establishment of some specific options on how best to achieve confidentiality, integrity and availability of confidential information, in environments where data is being aggregated, where separation is underpinned by logical methods (e.g. virtualisation), and where attribution/traceability of activity may be challenging.

18.3 To develop a positive proposition for ICT specialists, and a roadmap that will enable existing practitioners to lead the way in the transition to Cloud computing services

There need to be agreed methodologies, case studies and training to bring existing ICT practitioners on board with the transition to Cloud computing services. While some are open to experimentation and “learning through doing”, in some organisations it is probably the case that some are steering clear of Cloud computing on the basis that it is not fully understood, and therefore can be perceived as presenting something of a threat.

18.4 To establish how trusted cloud service brokerages can best be established.

Trust is critical, as is the ability to have credibility (and thus be "listened to") when dealing with very large-scale cloud services providers. This paper has suggested that industry associations could play a key role in the establishment of Cloud service brokerages, and research into this possibility would be welcome, and also into alternatives such as computer distributors, the open source movement etc.

18.5 To determine how best to agree the technical standards that are needed for full realisation of the potential benefits of Cloud computing

Technical standards are needed in multiple areas, for example:

- to allow interoperability between cloud services, including resource pooling and burst capability.
- to enable automation of the selection, provisioning and management of a portfolio of cloud services for user organisations.
- to reflect best practice on ensuring reliable business service delivery, specifically achieving reliability, putting in place appropriate reporting, measurement and monitoring tools, and minimising vulnerability to major failures.

Competing interests

The author declares that he has no competing interests.

Authors contribution

Martin Bellamy was seconded into the Cabinet Office as director for the G Cloud programme between June 2009 and May 2010. He designed the overall approach to the research, and built support across the ICT industry and government departments for the formation of a multidisciplinary volunteer-based team. Having secured the necessary resources, Martin designed the research structure comprising the eight work strands, and set the terms of reference for each. He chaired the G Cloud programme team that moderated the contributions of each of the work strands into a cohesive proposition. He also oversaw production of the Service Specification, Transition Strategy, Founding Principles and business case.

In June 2010 Martin joined the National Offender Management Service as Change and ICT Director, and since April 2011 has also been a Crown Commercial Representative at the Cabinet Office. Martin has remained a member of the G Cloud Delivery Board. Martin has proactively initiated and participated in studies of how Cloud computing services can be used in NOMS.

Bibliography

[1] An article in Network World3 validated that the adoption of Cloud computing can lead to dramatic cost savings. Geir Ramleth, CIO of Bechtel www.webtorials.com/main/resource/papers/.../service-orchestration.pdf

[2] Above the Clouds: A Berkeley View of Cloud computing *Michael Armbrust Armando Fox Rean Griffith Anthony D. Joseph Randy H. Katz Andrew Konwinski Gunho Lee David A. Patterson Ariel Rabkin Ion Stoica Matei Zaharia* Electrical Engineering and Computer Sciences University of California at Berkeley 10Feb2009

[3] Assisting business process design with configurable processor fragments. Assy, Nguyen, Gaaloud (Telecom SudParis, France). IEEE Services Computing. June 2013 [5] http://www.rightscale.com/customers/iFixit-uses-rightscales-dynamic-autoscaling.php iFixit Uses

[4] http://www.eucalyptus.com/eucalyptus-cloud/iaas

[5] Huddle SaaS collaboration www.huddle.com/government/il3-security/

[6] http://www.policymic.com/articles/10526/amazon-crash-causes-instagram-and-netflix-to-blackout-is-cloud-computing-ready-for-prime-time Amazon Crash Causes Instagram and Netflix to Blackout: Is Cloud computing Ready for Prime Time?

[7] January 2012. Public cloud feasibility study (phase 2): management abstract from report of findings. Author Adrian Scaife, authorized by Ian Poree, Andy Nelson and Martin Bellamy. (Reports on a study that successfully delivered prototypes proving feasibility of using cloud services for implementing complex line of business processes for community sentences (Community Payback), that delivered a cost comparison, and reviewed information assurance issues. Concluded that it is technically feasible to use both public software as a service and infrastructure as a service cloud services to meet the business need, that the solution can be delivered for less than 50% of the cost of a conventional approach, but that the issues regarding information assurance/security are complex and that it was not possible to achieve sufficient traction to reach a definitive conclusion. The study concludes that the main challenges will be information assurance, integration (with existing systems), and culture, as it is more difficult to do something new where in house experience is limited and thus is not aligned with established processes)

[8] Gonzalez *et al. Journal of Cloud computing: Advances, Systems and Applications* 2012, 1:11 http://www.journalofcloudcomputing.com/content/1/1/11 A quantitative analysis of current

security concerns and solutions for Cloud computing Nelson Gonzalez1*, Charles Miers1,4, Fernando Reıgolo1, Marcos Simplıcio1, Tereza Carvalho1, Mats Na¨slund2 and Makan Pourzandi3 12 July 2012

[9] Trust as a facilitator in Cloud computing: a survey *Journal of Cloud computing: Advances, Systems and Applications* 2012, 1:19 doi:10.1186/2192-113X-1-19 Sheikh M Habib (sheikh.habib@cased.de) Sascha Hauke (sascha.hauke@cased.de) Sebastian Ries (riessebastian@googlemail.com) Max Mühlhäuser (max@informatik.tu-darmstadt.de) 23 August 2012

[10] July 2012. Hype cycle for cloud services brokerage 2012. Gartner. Identifies three main categories of brokerage service; aggregation, integration and customisation.

[11] July 2012. GSA Federal acquisition services. Cloud brokerage. Request for information. https://www.fbo.gov/notices/0e4bbe369331309722bb4f6429c5f80a (The RFI sets the context of existing Cloud computing services frameworks that aim to offer public sector organisations procurement vehicles that save cost and time through the adoption of Cloud computing technologies. Cloud brokerage is considered as an alternative model for future cloud acquisition that can potentially further these goals.)

[12] http://inls525fall2011.web.unc.edu/files/2011/09/DavidWyld.pdf Moving to the Cloud: An Introduction to Cloud computing in Government

[13] 2012. Preparing for the cloudburst. Roger Camrass. http://www.rogercamrass.com/preparing-for-the-cloud-burst/

[14] http://googleenterprise.blogspot.co.uk/2010/09/ahold-goes-google-international-food.html Ahold goes Google: International food retailer moves 55,000 employees to Google Apps

[15] http://googleenterprise.blogspot.co.uk/2012/01/bbva-banks-on-google-apps.html BBVA case study on Google Apps

[16] http://www.salesforce.com/showcase/stories/japanpost.jsp Case study on Japan posts use of salesforce.com.

[17] http://www.cloudbook.net/directories/gov-clouds/gov-program.php?id=100018 G-Cloud The UK Government's CIO, John Suffolk, announced the establishment of a UK onshore, private Government Cloud computing Infrastructure called G-Cloud.

[18] Investigating Decision Support Techniques for Automating cloud Service Selection Miranda Zhang1, Supervised by: Rajiv Ranjan1, Armin Haller1, Dimitrios Georgakopoulos1, Peter Strazdins Information Engineering Laboratory, CSIRO ICT Centre

[19] http://www.cabinetoffice.gov.uk/sites/default/files/resources/01-G-CloudVision.pdf DATA CENTRE STRATEGY, G-CLOUD & GOVERNMENT APPLICATIONS STORE PROGRAMME PHASE 2PHASE 2 SCOPE REPORT

[20] March 2012. The UK government launches its G Cloud store, but this is just the start. Andrea Di Maio. http://www.gartner.com/id=1944715

[21] Gonzalez *et al. Journal of Cloud computing: Advances, Systems and Applications* 2012, 1:11 http://www.journalofcloudcomputing.com/content/1/1/11 A quantitative analysis of current security concerns and solutions for Cloud computing Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho, Mats Na¨slund and Makan Pourzandi 12 July 2012

[22] http://www.bbc.co.uk/news/business-16486796 BBVA's director of innovation, Carmen Herranz, stressed that all customer data and other key banking systems would "stay in our own data centres" and be completely separate from the cloud solution.

[23] ITIL by Vernon Lloyd.
http://www.swetswise.com/FullTextProxy/swproxy?url=http%3A%2F%2Fitnow.oxfordjournals.org%2Fcgi%2Freprint%2F45%2F3%2F28.pdf&ts=1393178127315&cs=2368467170&userName=8080273.ipdirect&emCondId=103713&articleID=35563278&yevoID=2187676&titleID=393352&remoteAddr=129.31.241.61&hostType=PRO

[24] http://www.crn.com.au/News/255586,amazon-ec2-suffers-huge-outage.aspx/0 Amazon EC2 suffers huge outage *Brett Winterford on Apr 27, 2011 8:54 AM*

[25] May 2010. G Cloud information assurance work stream report. The authors G Cloud information assurance team, moderated by G Cloud programme team and G Cloud program director.

[26] G Cloud Technical Architecture Workstrand Report
http://www.cabinetoffice.gov.uk/sites/default/files/resources/08-G-CLOUD-TechnicalArchitectureWorkstrand-Report.pdf

[27] February 2010. G Cloud programme service management, organisation and governance

approach. http://www.cabinetoffice.gov.uk/sites/default/files/resources/06-G-CLOUD-ServiceManagement-OrganisationandGovernance-Approach.pdf

[28] September 2011. Cloud computing: security, market development and prospects for the G Cloud. Martin Bellamy. Westminster e forum.

[29] October 2011. Government cloud strategy. HM government http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf

[30] http://gcloud.civilservice.gov.uk/about/sales-information/ G Cloud sales information

[31] http://gcloud.civilservice.gov.uk/category/commercial/ G Cloud ii framework

[32] August 2012. Barriers to adoption of the cloud. University of Liverpool and MSc dissertation prepared by Ian Turner;- includes interviews with nine senior ICT practitioners from the government and supplier communities.

[33] October 2012. NOMS business challenges and cloud opportunities. Presentation by Martin Bellamy on learnings to date from deploying cloud services within the National Offender Management Service.

[34] Cooperative Expendable Micro-Slice Servers (CEMS): Low Cost, Low Power Servers for Internet-Scale Services James Hamilton Amazon Web Services 1200 12th Ave. S. Seattle, WA 98144 4th Biennial Conference on Innovative Data Systems Research (CIDR) January 4-7, 2009, Asilomar, California, USA.

[35] http://www.skyscapecloud.com/wp-content/uploads/Skyscape-UK-Public-Sector-Cloud-Prediction-2012-survey-results.pdf UK Public sector cloud survey 2012

[36] October 2012. “Hosting gov.uk to cost GDS record-breaking £600,000”. Article in Computerworld identifying the benefits of sourcing hosting services for the gov.uk site from the cloud store framework

[37] Rackspace www.rackspace.co.uk/managed-hosting/hosting-solutions/service-levels/

[38] Study by Hurwitz and Associates on ownership costs for NetSuite (http://www.nxturn.com/downloads/TheCompellingTCOCaseforCloudComputing.pdf)

[39] Business Application Acquisition: On-Premise or SaaS-Based Solutions? Bibi, S.; Katsaros, D.; Bozanis, P. Software, IEEE Volume: 29 , Issue: 3 Topic(s): Computing & Processing

(Hardware/Software) Digital Object Identifier: 10.1109/MS.2011.119 Publication Year: 2012 , Page(s): 86 – 93

[40] European business review titled “understanding the business impact of Cloud computing”, Wilcox, Venters, Whiteey and Hindle (Ref:http://www.europeanbusinessreview.com/?p=4587)

[41] Ravi Kalakota and Marcia Robinson “e business 2.0-a roadmap for success” 2001.

[42] http://www.economist.com/node/17730360 Why do firms exist? Ronald Coase, the author of “The Nature of the Firm” (1937)

[43] Bechtel Harnesses the Cloud: Case Study of an Enterprise Cloud http://cloudstoragestrategy.com/2009/03/bechtel-harnesses-the-cloud-a-case-study-in-service-delivery.html

[44] Perfect competition : Economics online http://www.economicsonline.co.uk/Business_economics/Perfect_competition.html

[45] CBI's Open Access report shows how open public service markets can lead to an increase in quality, choice and value for money http://www.cbi.org.uk/business-issues/public-services/open-access-report/

[46] The Innovator's Dilemma: Clayton M. Christensen

[47] February 2010. http://www.cabinetoffice.gov.uk/sites/default/files/resources/03-G-Cloud-SOC.pdf G Cloud program strategic outline business case. Authors G Cloud programme team.

[48] FedRAMP -- Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services http://www.gsa.gov/portal/category/102375

[49] A framework for ranking of Cloud computing services Saurabh Kumar Garg’ Steve Versteeg, Rajkumar Buyya http://www.buyya.com/papers/RankingClouds-FGCS.pdf

[50] A CIO primer on Cloud Services Brokerage Benoit J. Lheureux Daryl C. Plummer Neil Wynne Bill Caffery James D. Buckner Ian Beazley http://www.gartner.com/id=2201415

[51] Amazon EC2 - Amazon Web Services aws.amazon.com/ec2/

[52] G Cloud Phase 2 Commercial Strategy Report. May 2012

[53] http://www.cio.co.uk/news/3272383/sita-airline-specialist-launches-first-community-cloud/

[54] G Cloud founding principles

[55] NOMSnet closure project report. Catherine Hamill, 2012

[56] MoJ guide to buying on G Cloud, published August 2012

[57] Internal report titled "Cloud Deployment Review", issued in May 2012, author David Caradine

[58] US government "Cloud Buyers Guide"; produced to support the US "cloud first" policy

[59] Cloud Standards Wiki http://cloud-standards.org/wiki/index.php?title=Main_Page

[60] Amazon: Some data lost in cloud outage is not recoverable http://www.bizjournals.com/seattle/blog/techflash/2011/04/Amazon-says-some-data-lost-in-cloud.html?page=all

[61] NIST Cloud computing standards roadmap http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf

[62] How the Cloud Computing Paradigm Could Shape the Future of Enterprise Information Processing Amin Anjomshoaa & A Min Tjoa Vienna University of Technology
http://delivery.acm.org/10.1145/2100000/2095700/p7-anjomshoaa.pdf?ip=129.31.241.61&id=2095700&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1C71412BEE85F14E563EADB9F9F3FF4A5&CFID=295044466&CFTOKEN=76495270&__acm__=1393082760_dd4278809e3517aff12d0b61a0478540

[63] IT Auditing for Modern Technology Management Charles H. Le Grand
http://www.tandfonline.com/doi/full/10.1080/07366981.2013.795047#.UwjDJP1KOFI

[64] Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment Subhas Chandra Misra Arka Mondal1
http://www.sciencedirect.com/science/article/pii/S089571771000155X

[65] Risk perception and risk management in cloud computing: Results from a case study of Swiss companies Nathalie Brender1, Iliya Markov
http://www.sciencedirect.com/science/article/pii/S0268401213000753

[66] Google and Amazon will be key future cloud suppliers
http://www.computerweekly.com/news/2240089299/Google-and-Amazon-will-be-key-future-cloud-suppliers

[67] How bad tech is costing companies -- Uninspired or outdated workplace technology has led to the rise of a BYOD culture -- bring your own device -- and, with it, risks to security.
http://money.msn.com/investing/how-bad-tech-is-costing-companies

[68] The Number Of Smartphones In Use Is About To Pass The Number Of PCs HENRY BLODGET
http://www.businessinsider.com/number-of-smartphones-tablets-pcs-2013-12

[69] The pricing model of cloud computing services, Dan Ma, Jianhui Huang
http://dl.acm.org/citation.cfm?doid=2346536.2346586

[70] Winds of Change: From Vendor Lock-In to the Meta Cloud
Benjamin Satzger, Waldemar Hummer, Christian Inzinger, Philipp Leitner, and Schahram Dustdar • Vienna University of Technology
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6415917

[71] Information Technology Industry http://www.qfinance.com/sector-profiles/information-technology

[72] Cloud computing: the nexus of strategy and technology
Peter Ross and Michael Blumenstein
http://www.emeraldinsight.com/journals.htm?articleid=17093347&show=abstract

[73] Evaluating cloud deployment scenarios based on security and privacy requirements
Christos Kalloniatis • Haralambos Mouratidis • Shareeful Islam
http://download.springer.com/static/pdf/110/art%253A10.1007%252Fs00766-013-0166-7.pdf?auth66=1393268469_69b4cd6b96abba0e64162370e2445fc1&ext=.pdf

[74] Cloud Computing: Security and Reliability Issues
Farhad Ahamed, Seyed Shahrestani and Athula Ginige

University of Western Sydney, School of Computing, Mathematics and Engineering, Sydney, Australia.
http://www.ibimapublishing.com/journals/CIBIMA/2013/655710/655710.html

[75] Cloud monitor Giuseppe Aceto Alessio Botta Walter de Donato Antonio Pescap http://www.sciencedirect.com.iclibezp1.cc.ic.ac.uk/science/article/pii/S1389128613001084?np=y

[76] Toward Cloud Computing Reference Architecture: Cloud Service Management Perspective Yanuarizki Amanatullah, Charles Lim, Heru Purnomo Ipung, Arkav Juliandri
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6588059

[77] Common models in SoA
http://www1.unece.org/stat/platform/download/attachments/65372409/common_model_in_soa_wp.pdf?version=1

[78] Towards Secure Cloud Bursting, Brokerage and Aggregation
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5693261
Srijith K. Nair1*, Sakshi Porwal2, Theo Dimitrakos1, Ana Juan Ferrer3, Johan Tordsson4, Tabassum Sharif5, Craig Sheridan5, Muttukrishnan Rajarajan6 and Afnan Ullah Khan1

[79] Cloud Computing
EU cloud computing strategy for better standards, safer contracts and more cloud in the public and private sector. (more about cloud computing)
http://ec.europa.eu/digital-agenda/cloud

[80] Service-Oriented Cloud Computing Architecture Wei-Tek Tsai*, Xin Sun, Janaka Balasooriya
http://staff.fit.ac.cy/com.bd/MIS/Readings/Service-Oriented%20Cloud%20Computing%20Architecture.pdf

[81] Hansard House of Commons Record from Wednesday 8 February 2012
http://www.publications.parliament.uk/pa/cm201212/cmhansrd/cm120208/debtext/120208-0001.htm

[82] Delivering 21st-century ICT for the National Health Service

http://www.ehi.co.uk/insight/analysis/905/horrible-history-part-one:-here-comes-the-21st-century

[83] Government ICT strategy
http://webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/317444/ict_strategy4.pdf

[84] Cloud Computing in E-Government across Europe A Comparison
Bernd Zwattendorfer1, Klaus Stranacher1, Arne Tauber1, and Peter Reichstädter2
E-Government Innovation Center (EGIZ), Graz University of Technology, Graz, Austria
{bernd.zwattendorfer,klaus.stranacher,arne.tauber}@egiz.gv.at E-Government / ICT Strategy at Austrian Federal Chancellery, Vienna, Austria
peter.reichstaedter@bka.gv.at

[85] Australian government cloud computing strategy
http://www.finance.gov.au/cloud/

[86] Exploring the Cloud - A Global Study of Governments ... - KPMG
www.kpmg.com

[87] State of Cloud Computing in the Public Sector – A Strategic analysis
www.frost.com/prod/servlet/cio/232651119

[88] Canadian Government Cloud Computing - Canada
Cloudcanadacloud.files.wordpress.com/ 2012/01/govcloudcanada.pdf

[89] New Zealand government cloud computing strategy
http://ict.govt.nz/programmes/government-approach/

[90] Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker http://www.defense.gov/news/disadesignation.pdf

[91] Cloud Computing Reference Architecture, September 2011 – NIST
www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[92] Economics, by David Begg, Stanley Fischer and Rudiger Dornbusch, Chapter 10, published by McGraw-Hill

[93] Oligopoly pros and cons
http://www.buzzle.com/articles/advantages-and-disadvantages-of-oligopoly.html

[94] Competition Policy Analysis
Einar Hope Hoboken : Taylor and Francis 2002.
Chapter 8: Competition policy in the information economy (Carl Shapiro)

[95] The Economics of Cloud Computing Federico Etro

[96] Corporate Turnaround by Stuart Slatter, David Lovett © Penguin UK

Annex 1: Paper and slides presented on 27 June 2013 to
IEEE 2013 International Workshop on Services Discovery and Composition, Santa Clara, CA

Adoption of Cloud Computing services by public sector organisations

The opportunity for cloud services brokerages to help overcome barriers to mainstream deployment

Martin Bellamy
Department of Computing, Imperial College (part time)
National Offender Management Service, Ministry of Justice
London, UK
m.bellamy09@imperial.ac.uk

Abstract—**Despite attractive benefits a range of barriers is inhibiting take-up of Cloud Computing services which in many organisations remains at less than 5% of the ICT footprint. The generic factor inhibiting wider deployment is that use of Cloud Computing services can expose organisations to heightened risks, particularly where business critical processes and sensitive data are involved. While the inherent risks can be managed, in the near term significant investment in skills, processes, tools and technology is a prerequisite for doing so efficiently. For many organisations that use ICT services, the level of investment needed will often be prohibitive. This has created the opportunity for the emergence of trusted cloud brokerage services that can invest strategically to assist organisations with the use of Cloud Computing services and management of the associated risks, developing service portfolios that reduce upfront costs, so that use of Cloud Computing services becomes the best choice on a project by project basis. This paper considers the benefits of Cloud Computing, identifies the barriers to take up and how these can be overcome, and considers how cloud services brokerages can potentially develop new capabilities to accelerate take-up and benefits realisation.**

Keywords- Cloud Computing, distributed systems, service orientated architecture

INTRODUCTION

The potential benefits of using Cloud Computing services include cost savings, faster innovation, delivery of modern services that meet consumers' expectations, and improved choice and affordability of specialist services. It has been estimated that large automated data centres located near to low-cost power supplies can reduce the unit costs of producing ICT based services by over 80% [1], compared to conventional approaches.

While the benefits of using Cloud Computing can quickly seem attractive, the need for new skills and processes, and the many risks that need to be overcome are inhibiting take-up. Public sector organisations may conclude that the overheads that will be incurred either exceed the benefits, or will lead to unacceptable delay. The range of issues that need to be considered is broad, particularly security and legal obstacles, with a recent paper identifying 26 discrete challenges [2]. Even if all the specific questions can be addressed, there remains the challenge of establishing trust in the Cloud Computing supplier, with current trust models needing significant improvement for use in Cloud Computing contexts [3].

Recognising the potential benefits, in 2009 the then UK government CIO [4] asked the author to lead the G Cloud programme, initially to develop a strategy for Cloud Computing in the UK public sector. The approach adopted was to form a volunteer-based programme team consisting of representatives from both public sector organisations and the Information and Communications Technology (ICT) industry. In total over 100 individuals contributed over a six month period, organised into several work strands, coordinated by a programme board that was chaired by the author. This paper considers the work done by the G Cloud programme between 2009 and 2013; the findings are also relevant to organisations in the private sector.

A key contextual characteristic is that in mature economies, the majority of public sector ICT costs relate to the provision of services to citizens. Services, for example "register a birth" and "submit a tax return" are delivered by a wide variety of organisations, and are typically developed and managed independently. While each service is to some extent unique, most also comprise elements that could be sourced from commodity Cloud Computing suppliers.

Creating integrated proprietary "line of business" processes from commodity services will typically involve sourcing multiple cloud services, integrating these with in-house services, addressing end-to-end security and service management requirements, and putting in place ongoing arrangements to ensure service continuity. This is particularly complex in a context that involves multiple providers, working to different SLA's, with different upgrade cycles, and who are competing to innovate potentially with focus on different market segments.

POTENTIAL BENEFITS

While the potential for cost reduction is often the first benefit cited for Cloud Computing services, we found that careful analysis is needed in each case. Although the "list price" of Cloud Computing services may appear low compared to current ICT costs, it is essential to ensure a like-for-like comparison is done. For example configuration and data migration costs are typically not included.

The benefits of using Cloud Computing services often extend well beyond cost reduction and can include:

- faster ability to implement innovative customer offerings, with much reduced initial costs,

- access to value adding capabilities such as collaboration tools and social networking may come at no extra cost within a service, and
- the ability to deliver to mobile devices with rich user interfaces, and a range of tools such as integrated mapping, can enable rapid "catch up" with users' expectations of what modern workplace ICT should be providing.

We identified that together, the combination of tools that enable organisations to work more effectively, and those that can accelerate delivery of market leading customer propositions can boost the pace of business innovation.

G CLOUD VISION;- A FRAMEWORK FOR SYSTEMATIC DEPLOYMENT OF CLOUD COMPUTING SERVICES

The G Cloud vision [5] sought to establish a framework for systematic deployment of Cloud Computing services intended to realise the benefits of Cloud Computing while managing the associated risks. Developed by the G Cloud programme team, it called for public sector bodies to switch from a "business solution orientated" model to a "commodity services procurement" approach for new ICT. Public cloud services would be used in preference to those specifically built for government, with services advertised through an online application store (now launched as CloudStore [6]), with transparent pricing that reduces as service usage volumes increase.

Cloud Computing can expose organisations to additional risks, primarily because it involves placing organisational information into shared resources that are managed and controlled by third parties. Potential threats thus arise from:

- Cloud Computing suppliers,
- other users of the Cloud Computing service,
- third parties illicitly circumventing access controls and protection to obtain access via the Internet.

Studies have concluded that while the inherent risks not new, the Cloud Computing model does potentially intensify their impact [7]. The commodity supplier orientation of cloud providers means that customer support is typically conducted via email through a website with standard SLAs and contractual terms. The large suppliers wield considerable market power, and thus customers of Cloud Computing suppliers may have comparatively little influence and can find it hard to get attention if things go wrong. Such risks are likely to be heightened where the cloud provider (and it's contracts) are based in a different country and thus legal jurisdiction.

We considered that from the perspective of governments, there are four main categories of risk inherent in using Cloud Computing services [8]; Inability to maintain confidentiality, integrity and availability of information, loss of control of information service design, inability to assure service characteristics, and vendor lock-in potentially leading to exploitative behaviour.

Inability to maintain confidentiality, integrity and availability of information (Information Assurance)

When using a third-party cloud provider, confidence that an organisation's data will be available when needed and not inappropriately disclosed to a third party depends on a combination of robust technical, procedural and personnel controls. Whether these have all been developed and applied effectively cannot be verified without extensive dialogue with the vendor, and with a cloud service this is often impractical. Establishing trust in a context where there is not a personal relationship between vendor and customer, and where there is no regulation or agreed industry standards, presents a real challenge.

Cloud services are often provided on a global basis, and data, or user identity verification information may flow outside national borders. It's important to understand any legislative requirements such as the need to keep data within a particular geography, and to ensure the cloud provider is able to fulfill these.

Loss of control of information service design.

Cloud providers innovate through the addition of new features; generally these are prioritised by the provider to optimise market share and future profit. From the perspective of a specific user organisation, this creates the possibility that services selected as they currently meet business needs cannot be guaranteed to continue to do so in the future.

Inability to assure service performance.

Some cloud providers provide service guarantees that are based on assumptions on the peak simultaneous usage level generated by customers. Should this be exceeded service degradation occurs, with many providers then offering a rebate of charges. While financial compensation alone may be acceptable for some services, this is not the case for services that are genuinely business critical. Hence the attributes to consider include services' design resilience, as well as factors such as failure recovery time, whether a disaster recovery facility exists and fault resolution SLAs.

Vendor lock-in potentially leading to exploitative behaviour.

From the buyer's perspective, there would ideally be a "perfectly competitive market" for Cloud Computing services. However while Cloud Computing represents a step towards the 'perfect market' ideal, today there are significant shortfalls including a lack of consistency of services, significant entry and exit barriers (ie switching costs), and potentially high transaction costs where users need to seek to change lengthy "click to accept" contracts.

RISK MITIGATION

Mitigating the risks involved in using Cloud Computing services is challenging. It is relatively straightforward where Cloud Computing services are being used in isolation for services where the risks arising from data loss are comparatively low.

The challenges are greater when using Cloud Computing services to implement organisation specific "line of business" processes. As such processes are usually unique to the commissioning organisation, and will require access to sensitive internally held data, there will (by definition) not be immediately available Cloud Computing services that are "ready to use". Nevertheless

if may still be possible to build a "better" version of an existing process, and to deliver this at lower cost by using a combination of commodity Cloud Computing services that have been configured and integrated (usually with internal services) to meet the specific business need.

We identified that the number of "moving parts" means that the costs of identifying, evaluating and managing the use of Cloud Computing services for "line of business" processes can be prohibitive for consuming organisations. As these overheads will tend to increase over time given the growing range and diversity of Cloud Service providers, we concluded that this will be best overcome by coordinated standard-setting, selection, evaluation, assurance and accreditation.

Hence we proposed the establishment of the G Cloud Authority (effectively an internal cloud services broker) that would coordinate a managed and assured internal marketplace of services that public sector organisations can trust. We proposed that such services should be made available to public sector organisations via an on line portal; this was launched in 2012 as the CloudStore.

MANAGING INFORMATION ASSURANCE RISKS

We found that the transition to Cloud Computing services potentially brings benefits as well as risks from the Information Assurance perspective [8]. The risks include there being less, if any, control over changes made by the Cloud Computing provider. Additionally the concept of using virtualisation technology to support multiple organisations and their information on the same physical device is relatively new and is not regarded as highly secure, as there may still be security vulnerabilities that have not yet been discovered. There is also the commercial reality that some Cloud Computing providers prioritise features and early delivery to the market over and above exhaustive information security validation.

The potential benefits (from the Information Assurance perspective) of using shared Cloud Computing services include that the organisation overall needs to assure fewer services and thus increased assurance effort can be expended on each.

While the core information assurance risks of loss of confidentiality, integrity and availability remain unchanged, the global nature of some cloud service providers means there is less control over where data resides. With many services data will quite possibly end up outside national borders, potentially including countries that may be regarded as "higher risk". This in turn may bring new risks such as employees being vetted to different levels, potential interference by overseas governments and the possibility of inadvertent breach of legislation that restricts where data can be held.

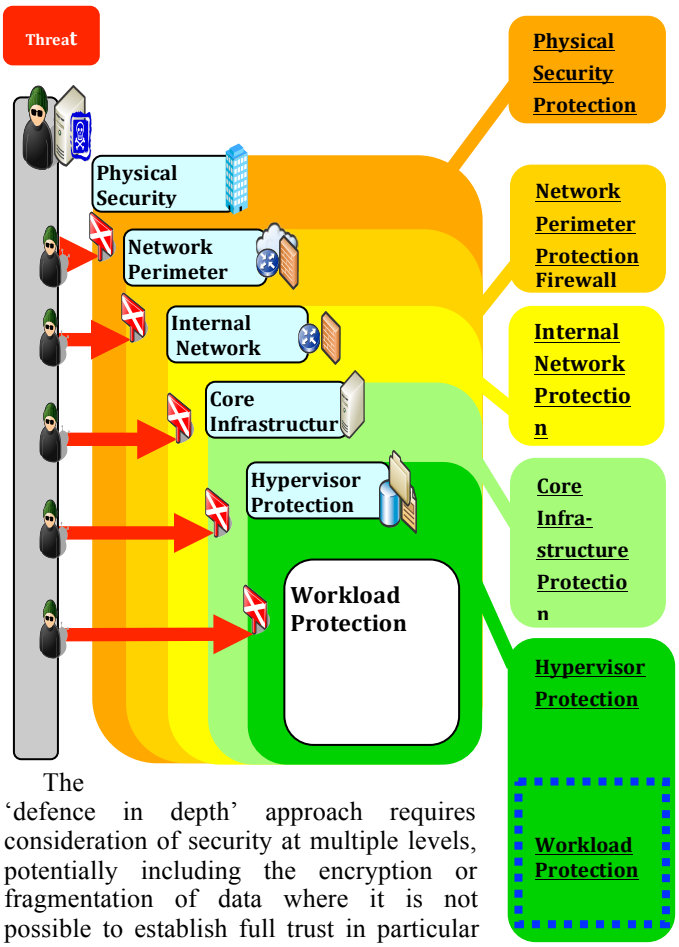
Before each deployment organisations will additionally need to consider the specific context of the service, the inherent information risks and the needs of the user community. This requirements setting process will need to be done on a case-by-case, organisation by organisation basis.

When selecting Cloud Computing Services consuming organisations will also need to consider a range of supplier information assurance issues including:

- user and employee access control,
- protective monitoring,
- forensic readiness (collection of digital evidence),
- clarity on roles and responsibilities,
- having a security incident management policy,
- organisational standards for data encryption, both "at rest "and "in-flight", and
- a sanitisation policy to ensure that data is securely removed when use of cloud service ceases.

We advocated the adoption of a 'defence in depth' approach that is depicted in Figure 1 below:

Figure 1: Depiction of "defence in depth" approach for cloud services information assurance.



The 'defence in depth' approach requires consideration of security at multiple levels, potentially including the encryption or fragmentation of data where it is not possible to establish full trust in particular providers. Organisations will need to consider their information risk appetite, and put into place processes to ensure that this is taken into account when setting the strategy for the selection and use of Cloud Computing services.

MITIGATING THE RISK OF LOSS OF CONTROL OF INFORMATION SERVICE DESIGN

The G Cloud programme technical architecture work-strand [9] reviewed areas where technical standards and policies may be needed to enable cohesive use of Cloud Computing Services. We identified that the areas for consideration within:-

- Infrastructure as a Service (IaaS) are data centre, networking, physical servers and virtualisation,
- Platform as a Service (PaaS), are the IaaS layers and additionally the operating system and

optionally other platform and infrastructure software, and

- Software as a Service (SaaS), are the PaaS and IaaS layers and the application layer (which is the only layer visible to the consumer).

This is illustrated in figure 2 below:

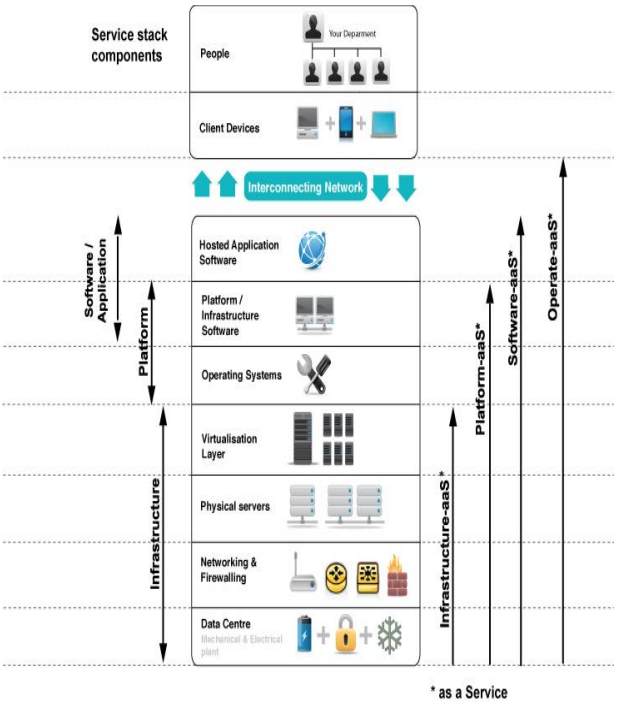


Figure 2: Cloud Computing service layers (IaaS, PaaS, IaaS)

To enable systematic use of SaaS services organisations may choose to define standards and policies for:

- data services, to provide a common secure interface to corporate data,
- a certified components repository; approved services that can be hosted on IaaS services,
- an online catalogue to allow end users to browse and select services,
- operate as a service, a set of services to assist with management and support of the services portfolio chosen by a user organisation, and
- interchange and transaction services, to allow secure, auditable interconnections to be made between cloud services, and multi-stage transactions to be managed involving successful end to end use of a series of services.

Services Orientated Architecture and integration capability

The majority of public sector ICT costs relate to the provision of services to citizens, and this in turn involves many hundreds of relatively complex business services. Examples include "apply for a driving test" and "claim state pension". The current ICT deployment model is to design the ICT enablers for such processes independently, and while all have some unique business logic, the majority comprise common elements such as "authenticate citizen", "capture data", "produce secure document", "collect payment" and "make payment". We identified the potential for improved outcomes and substantial savings by moving to a model where each of the common services is developed through a managed process, with two or three pan-government sources of supply of each. Such services could then be described in the catalogue, and made available for integration into the business specific processes of each organisation. This ambition is highly aligned with the principles of Service Orientated Architecture (SoA), with Cloud Computing providing an attractive hosting and delivery model that readily allows SoA based services to be shared across multiple organisations.

ASSURING SERVICE PERFORMANCE

We found that Cloud Computing presents new challenges for the ICT Service Management community [10]. In contrast to the established 'on premise' model, organisations that purchase Cloud Computing services have no control over providers' approaches to ICT Service Management, and have to rely on "good practice" being implemented. Further the commoditised "use as is" nature of Cloud Computing services means that it will often be necessary to use two or more together to achieve a particular business process outcome.

Given the limited control of any particular customer, it will not usually be possible either to access the engineering detail how the service has been constructed, or to fully model how the service will perform under various extreme scenarios. It is therefore necessary to rely on commitments and assurances made by the Cloud Computing vendor, with these potentially being verified by independent auditors.

Establishing trust in suppliers of Cloud Computing services is therefore essential. In the longer term some aspects of these risks may be mitigated if standards and market transparency develop to the point where "instantaneous transfer" to an alternative service becomes possible. Again therefore the implication is that consuming organisations will need to ensure that significant discovery and validation work has been undertaken with each cloud provider before adopting services for business critical processes.

Where a cloud service is being used together with internal services, or where several cloud services are being used together, there will be a need for a "service integrator" accountable for achieving a predictable end to end service outcome for business users. Methodologies will be required that build on the SLAs of each service provider. Standards for Service Management would be of benefit to service integrators in predicting, measuring and sustaining service outcomes. Currently there is a lack of maturity in this area; while the IT infrastructure library (ITIL) provides a possible framework, it was specified with conventional ICT delivery in mind, and is not consistently deployed across organisations.

In the near-term organisations will need to ensure that there is a framework for managing Cloud Computing services, and that this is taken into account in developing the approach for sourcing, governance, procurement and measurement. This framework will need to recognise that the more sophisticated and embedded in the business a service is, the greater the range of service management

activities that will be needed. This concept is depicted in Figure 3 below:

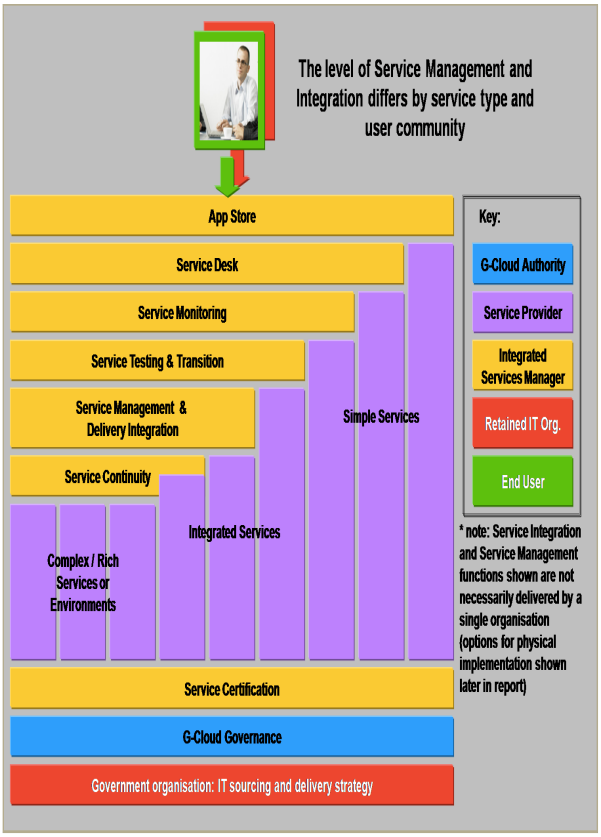


Figure 3: Relationship between complexity of cloud services and intensity of service management engagement

New Service Management tooling will also be required; for example so that the helpdesk can maintain a "service dashboard" providing a holistic view of the information services their organisation is providing (internal and external), encompassing those that include Cloud Computing services

G Cloud announcement

We announced the imminent publication of the UK government cloud strategy at the Westminster eForum on September 13, 2011 [12]. The G Cloud strategy (Cloud Computing) was then published in October 2011 [13]. The strategy embodies the core principles of the vision that was developed by the G Cloud programme team in 2009/10. It prioritises those aspects that can be progressed with lower expenditure and which maximise early benefits.

The strategy reasserts the principles of Cloud Computing and puts in place a "public cloud first" policy. Specifically, the strategy positions the G Cloud as a hybrid cloud consisting of public, private and potentially community cloud services. It sets the expectation that the G Cloud will be an assured collection of services that will grow over time, rather than being a single entity.

The anticipated benefits comprise cost reduction and increased business flexibility. Targets for the take-up of cloud services are set.

It is recognised that changing the way government buys ICT is fundamental to achieving the desired benefits. Thus the strategy acknowledges the need for both behavioural change and development of the supplier marketplace (which will take time) and which can be aided by the establishment of a G Cloud Authority (that could provide some cloud brokerage capabilities).

Progress one year after publishing the G Cloud strategy

Following a procurement process, CloudStore was launched in April 2012 [11] as an online catalogue for accessing both public and community cloud services that have undergone initial supplier and service accreditation [12]. By end March 2013 there had been c1,000 purchases from CloudStore, equating to sales of just over £18 million [13].

A significant increase in the range of services available was announced with the G Cloud iii framework in May 2013 [14]. Over 700 suppliers are now on the framework demonstrating substantial market interest and commitment. It is also notable that the use of CloudStore significantly opens up opportunities and reduces overheads for suppliers in selling ICT based services to government. This in turn has enabled small and medium sized enterprises (SMEs) to play a significant role; capturing in the region of 70% of the sales to date. As CloudStore becomes better established, this has the potential to drive a marked change in the supplier landscape, enabling new entrants to capture significant volumes of business that would previously have gone to well-established sources of supply.

As expected, the majority of CloudStore purchases have been for relatively "self-contained" services. Popular services have thus been those such as:

- web hosting,
- office and collaboration software,
- storage as a service, and
- specialist cloud (support) services.

While momentum for such "self-contained" deployments continues to build, this is addressing only a relatively limited portion of large organisations' ICT needs. Further work is needed to determine and put in place the capabilities (both foundation services and the skillsets needed) to replace core "line of business" applications.

The G Cloud Authority has not been established as a separate entity; rather there is the realisation that standards, in particular security related standards, need to be aligned across all ICT infrastructure components; i.e. Cloud Computing services, hosting, network and end-user devices. Accordingly there has been active consideration of the formation of a single Public Sector Technical Services Authority to cover all areas of infrastructure standards

Barriers to cloud deployment

Several surveys of attitudes to cloud adoption were conducted amongst UK public sector organisations and suppliers in 2012 [15,16].

Overall, while there is acknowledgement of benefits such as flexibility, agility, lower costs and improved service levels from using cloud services, feedback from

the surveys cites perceived risks as slowing take-up. The top concerns are security, potential risks from using "unproven" technology, lack of control of data residency, and lack of a framework for building business cases.

There are also some significant 'soft' barriers [16]; for many practitioners (CIOs and their teams) Cloud Computing changes, and thus potentially threatens established roles. Specifically there is some concern that CIOs risk losing relevance and being bypassed, and that to mitigate this CIOs will need to demonstrate a greater contribution to business strategy and information management, setting the context where in house ICT teams can add value in the selection and management of Cloud Computing services. Achieving this however requires a change in culture and skills across the internal ICT organisation, and this needs to be led by the CIO and the senior team.

There is also the need for processes and methodologies that set out how to use cloud services to address specific business needs, and to mitigate what many currently see as unacceptably high levels of risk.

Technical issues are seen to present less of a barrier than people and process issues; the technical concerns include whether the inherent scalability of Cloud Computing services moves capacity risks to networks, which cannot scale as quickly. While there has been some research on potential mitigations to network constraints, such cloud like "capacity on demand" capabilities are not generally offered by network suppliers today. Hence, given that at peak times Cloud Computing service capacity can theoretically expand indefinitely there is a danger that the Wide Area Network (WAN) becomes the constraint. There is thus the risk that the use of dynamically scalable Cloud Computing services simply shifts the bottleneck from the datacentre to the network, and does not in fact improve performance for end-users.

There are also concerns on issues such as how to ensure applications design meets non-functional requirements in the cloud environment. Some have commented that there needs to be faster progress on setting standards.

In summary, to accelerate Cloud Computing deployment to address core "line of business" processes further work is needed on a range of issues including:

- security concerns,
- lack of clarity on legal issues,
- networking risks,
- lack of mature design and Service Management models,
- lack of governance frameworks that are relevant to Cloud Computing deployment, and
- lack of standards and in-house capability.

While suppliers' interest in the G Cloud initiative remains strong, some have found it challenging to meet accreditation requirements; these are based on ISO27001 and have been reduced to the essential minimum. The accreditation process covers a range of areas including security, service management and support, data location and vetting status of employees. Some suppliers have found it difficult to submit the quality of evidence expected, although there has also been feedback that the accreditation process has been helpful, and has resulted in some suppliers strengthening their security processes.

From the perspective of consuming organisations the process of identifying and selecting appropriate services can be a significant overhead, while core re-usable SoA type services such as "make payment" are still to emerge. In addition to the ICT community, adoption of Cloud Computing services requires active business leadership, and the involvement of commercial and other teams. It is also clear that the adoption of Cloud Computing services involves changes in working practices for quite a wide range of internal teams, and that there is scope for investing more effort in getting the entire organisation aligned in using Cloud Computing based approaches. Occasionally, typically where there has been a failure to adequately engage specific functions, Cloud Computing has been seen as a threat to the relevance of hard earned specialist knowledge. The risk is that some individuals or functions could block or delay implementation of Cloud Computing based services, and thus the realisation of benefits.

SOME EXAMPLES OF DEPLOYMENTS

The UK National Offender Management Service (NOMS] is responsible for the UK Prison and Probation services, organisations that together have over 60,000 employees. NOMS has considered Cloud Computing in a number of cases, resulting in the use of both public and private cloud services.

NOMS has successfully deployed public Cloud Computing services for collaboration and for provision of a shared interventions database. A private cloud approach has been adopted for development and test infrastructure services. The deployments to date are all relatively self-contained and do not involve particularly sensitive data. Deployments in general were straightforward, with the Cloud Computing services offering functional improvements over those previously used. In one case there was an unexpectedly large benefit from moving to a "pay per use" model. With costs per user now transparent and recharged to the consuming business units, there was a substantial reduction in business demand leading to a greater cost saving than had been anticipated.

A key learning point for the future is to ensure the capabilities of cloud services are used on an "as is" basis, with business needs negotiated where necessary to ensure there is a good fit. This follows an attempt made to replicate existing Management Information reports using the Cloud Computing service, which proved complex, resulting in a schedule overrun.

A NOMS initiative to explore the possibility of using public cloud services to implement a relatively complex organisational process proved less successful. This process had originally been selected as data would need to cross-organisational boundaries, and was thus theoretically as a good fit for Cloud Computing services. The evaluation found that the selected Cloud Computing services could:

- meet functional requirements in full,
- deliver additional benefits including an outstanding quality of user experience, and
- provide additional value adding features such as geolocation, mapping, and mobile device integration.

However there were difficulties in establishing confidence that information would be held sufficiently securely and would not be vulnerable to unauthorised access. Risks were heightened as the system interfaces to a large sensitive internal database. In the event it was not possible to proceed with the cloud solution as information assurance and compliance requirements could not be resolved within the business timescales.

THE POTENTIAL ROLE FOR CLOUD SERVICES BROKERS

The Cloud Computing business model reduces barriers to entry for ICT suppliers, and is thus leading to growth in the numbers of ICT suppliers, as well as a more diverse range of services. As previously discussed this creates a challenge for potential buyers of Cloud Computing services; how to understand what is available on the market, to validate whether services meet (and will continue to meet) business needs, and to build sufficient confidence in the supplier? With hundreds of service providers the challenge of conducting a rigorous market assessment is daunting.

The work done by the G Cloud programme in 2009/10 identified potential services to be provided by the G Cloud Authority. This is effectively a proposal for a brokerage capability. Its roles would include provisioning services once bought from the CloudStore, instantiating services with appropriate business data, and integrating the service's management tools into the buying organisation's service management framework. Additionally billing would be coordinated, avoiding the need to validate invoices from multiple cloud providers. It was recognised that a governance framework would be essential to coordinate multiple services into such an integrated framework.

Given the proliferation of Cloud Computing services, trusted cloud service brokerage services can add value in identifying and validating cloud services suitable for use by a particular organisation or business community. Such an approach can avoid costly duplication of assurance, and share the costs of managing the relationships with cloud suppliers and of providing integration and transaction management services. A central capability can also help expedite deployments when there are new business solution needs to be addressed.

It is clear that it will be critical for cloud services brokerages to establish their "trustworthiness". Reputation will help with this in time, but given the high dependence that organisations using cloud brokerages will have on these suppliers, it will be challenging for new entrants to convince user organisations that they will be safe partners to collaborate with, and that this will remain the case over the medium to long term. Establishing trust could potentially be accelerated through cloud services brokerages being commissioned by industry associations, who could then retain audit rights, as well as the mandate to transfer the business or introduce additional brokerage services in light of experience.

CONSIDERATIONS AND FUTURE WORK

Cloud Computing has potential to bring substantial benefits to organisations both through lowered ICT costs and increased affordability of specialist services. For these reasons the increasingly pervasive deployment of Cloud Computing services is inevitable.

In most organisations, initial Cloud Computing deployments will focus on replacing some commodity applications such as email and office software, however these do not generally have a significant impact on overall ICT costs. Progressing beyond this stage to use commodity Cloud Computing services for complex organisation specific "line of business" processes involves accepting and effectively managing different combinations and levels of risk.

The expertise needed for successful use of Cloud Computing services in "line of business" contexts include cloud service management and commercial skills, and Information Assurance capability. Additionally other "soft" barriers need to be addressed to accelerate delivery of the benefits of Cloud Computing;- for example leadership, culture, capabilities and processes.

Some organisations may conclude that overheads of acquiring the necessary skills, and that the costs of selecting, integrating and managing Cloud Computing services are prohibitive.

There is hence a market opportunity for cloud services brokerages to assist organisations in managing these issues. To do so efficiently brokerages will need efficient processes, automated where possible. Significant investment is thus needed in cloud services brokerages to deliver the potential of Cloud Computing. The "first movers" that succeed in overcoming the challenges in establishing comprehensive efficient cloud brokerage capabilities can expect to gain significant competitive advantage.

Deployment of Cloud Computing services into large-scale organisations represents a change journey that is likely to evolve over a period of more than a decade, with progress accelerating over time as the range of cloud services providers, and the numbers and capabilities of cloud services brokers together enable progressively more compelling "buy propositions" to be put to user organisations.

There is scope for further work to identify how trusted cloud services brokerages can best be established; trust is critical, as is the ability to have credibility (and thus be "listened to") when dealing with very large-scale cloud services providers. This paper has suggested that industry associations could play a key role in appointing and sponsoring cloud services brokerages, and research into this possibility (and also into alternatives) will be beneficial.

ACKNOWLEDGEMENTS

This paper draws on the work of the many contributors to the UK Government G Cloud programme over the period 2009 to 2013. I would particularly like to thank my supervisor at Imperial College, Professor John Darlington for his support and guidance.

AUTHORS CONTRIBUTION

Martin Bellamy was seconded into the Cabinet Office as programme director for G Cloud between June 2009 and May 2010. He designed the research approach, proposed and built support across the ICT industry and government departments for the formation of a multidisciplinary volunteer-based team, and designed the research team structure of eight work strands,

setting the terms of reference for each. He chaired the G Cloud programme team that moderated the contributions of each of the Phase 2 work strands into a cohesive proposition. He also oversaw production of the service specification, transition strategy and business case. Martin Bellamy joined the National Offender Management Service in June 2010 as Change and ICT Director, and has remained a member of the G Cloud Delivery Board. He has initiated studies of how Cloud Computing services can be used in NOMS. In 2009 Martin commenced a part time research PhD degree at the Department of Computing at Imperial College London. The opinions expressed are those of the author.

COMPETING INTERESTS

The author declares that he has no competing interests.

LIST AND SOURCES OF FIGURES

Figure 1: Depiction of "defence in depth" approach for cloud services information assurance [8]

Figure 2: Cloud Computing service layers (IaaS, PaaS, Iaas) [9]

Figure 3: Relationship between complexity of cloud services and intensity of service management engagement [10].

REFERENCES

[1] Above the Clouds: A Berkeley View of Cloud Computing Michael Armbrust Armando Fox Rean Griffith Anthony D. Joseph Randy H. Katz Andrew Konwinski Gunho LeeDavid A. Patterson Ariel Rabkin Ion Stoica Matei Zaharia Electrical Engineering and Computer Sciences University of California at Berkeley 10Feb2009

[2] Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11 http://www.journalofcloudcomputing.com/content/1/1/11 A quantitative analysis of current security concerns and solutions for ÇNelson Gonzalez1*, Çharles Miers1,4, Fernando Red ıgolo1, Marcos Simpl ıcio1, Tereza Carvalho1, Mats Na¨slund2 and Makan Pourzandi3 12 July 2012

[3] Trust as a facilitator in Cloud Computing: a survey Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:19 doi:10.1186/2192-113X-1-19 Sheikh M Habib (sheikh.habib@cased.de) Sascha Hauke (sascha.hauke@cased.de) Sebastian Ries (riessebastian@googlemail.com) Max Mühlhäuser (max@informatik.tu-darmstadt.de) 23 August 2012

[4] The UK Government's CIO, John Suffolk, announced the establishment of a UK onshore, private Government Cloud Computing Infrastructure called G-Cloud. http://www.cloudbook.net/directories/gov-clouds/gov-program.php?id=100018 G-Cloud

[5] Data Centre Strategy, G-Cloud & Government Applications Store Programme Phsae 2 scope report http://www.cabinetoffice.gov.uk/sites/default/files/resources/01-G-CloudVision.pdf

[6] March 2012. The UK government launches its G Cloud store, but this is just the start. Andrea Di Maio. http://www.gartner.com/id=1944715

[7] Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11 http://www.journalofcloudcomputing.com/content/1/1/11 A quantitative analysis of current security concerns and solutions for Cloud Computing Nelson Gonzalez, Charles Miers, Fernando Red ıgolo, Marcos Simpl ıcio, Tereza Carvalho, Mats Na¨slund and Makan Pourzandi 12 July 2012

[8] May 2010. G cloud information assurance work stream report. Authors G cloud information assurance team.

[9] G Cloud Technical Architecture Workstrand Report http://www.cabinetoffice.gov.uk/sites/default/files/resources/08-G-CLOUD-TechnicalArchitectureWorkstrand-Report.pdf

[10] February 2010. G cloud programme service management, organisation and governance approach. http://www.cabinetoffice.gov.uk/sites/default/files/resources/06-G-CLOUD-ServiceManagement-OrganisationandGovernance-Approach.pdf

[11] September 2011. Cloud Computing: security, market development and prospects for the G cloud. Martin Bellamy. Westminster e forum.

[12] October 2011. Government cloud strategy. HM government http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf

[13] http://gcloud.civilservice.gov.uk/about/sales-information/ G Cloud sales information

[14] http://www.publicservice.co.uk/news_story.asp?id=22874 Public sector told to buy IT through the cloud as G-Cloud iii goes live

[15] August 2012. Barriers to adoption of the cloud. University of Liverpool and MSc dissertation prepared by Ian Turner, involving interviews with nine senior ICT practitioners from the government and supplier communities.

[16] http://www.skyscapecloud.com/wp-content/uploads/Skyscape-UK-Public-Sector-Cloud-Prediction-2012-survey-results.pdf UK Public sector cloud survey

Martin Bellamy

Adoption of cloud computing services by public sector organisations

- The opportunity for cloud services brokerages to help overcome barriers to mainstream deployment -

Opportunity
When costs can be 80% lower why, in most large organisations, does cloud computing still account for less than 5% of the IT budget?

"Attractive in principle – difficult in practice"
-- organisations prioritise 'line of business' applications that are custom built, or configured, to reflect their unique business purpose.
-- cloud computing SaaS services do not immediately address organisations' unique business needs.
-- many needs can be addressed by using combinations of public cloud and internal services, but doing so robustly is costly.

Barriers to cloud deployment
Security
Design process
Operational management
Contractual concerns
Supplier management
Legal constraints
Resistance to change
Governance models
Standards

Solutions
Share the costs of addressing the challenges
via
Cloud Services Brokerages
Integrated Services Managers
Digital cloud marketplaces
Service Orientated Architectures



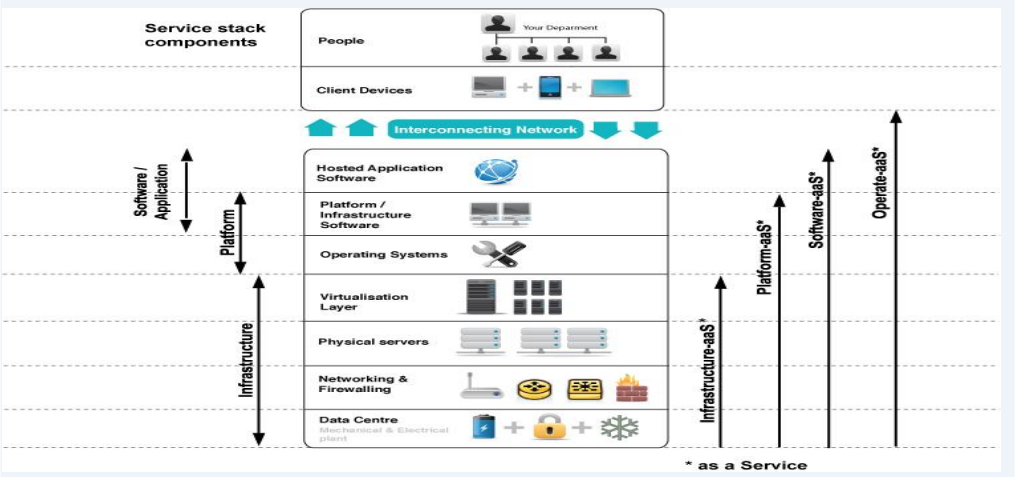
Establishing trust -- the critical success factor

"By March 2013, one year after launch, the UK Government CloudStore has 700 suppliers who have made 1,000 sales, with a combined value of £18 million"

Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk

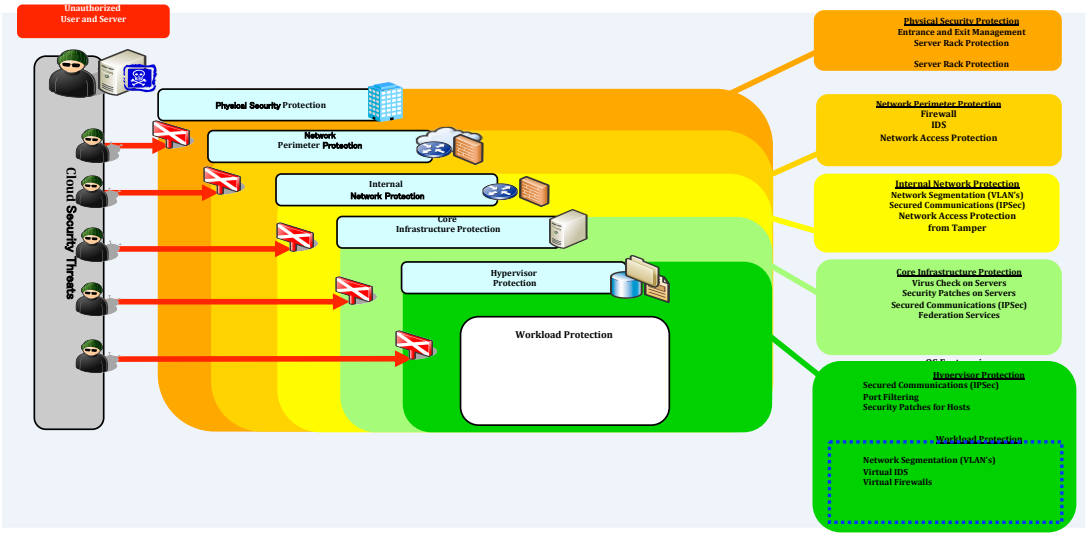
Cloud computing service layers



Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk

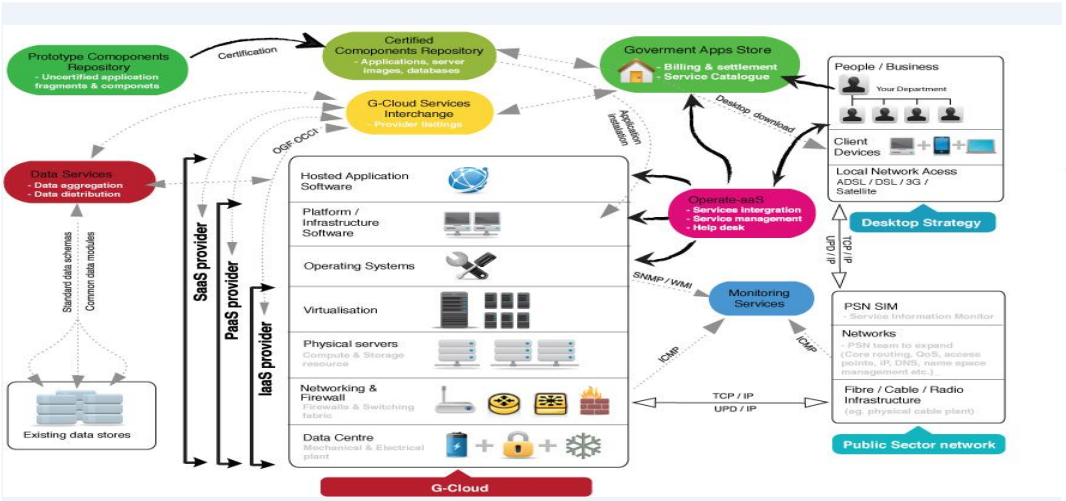
Information Assurance



Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk

Automating hybrid cloud creation



Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk

Using untrusted services

Customer/Citizen facing level – no persistent data

All services made available on multiple SaaS/PaaS providers

Orchestration and control level – holds user ids, access rights, keys

Controls 'who can access what' and decryption process
Likely hosted across IaaS providers or internally

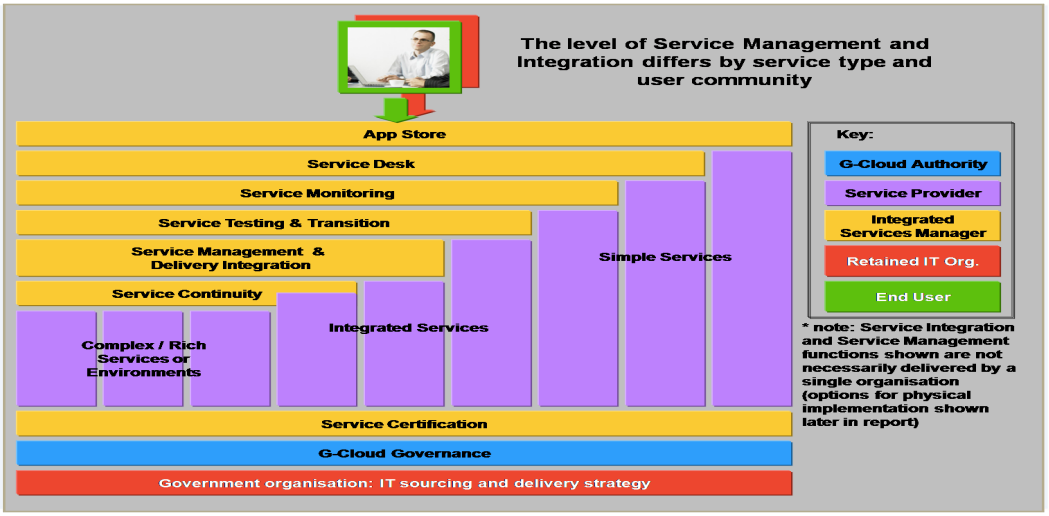
Back-end level – data and 'enterprise application' hosting

All data encrypted and held on multiple IaaS providers
All apps hosted on multiple IaaS providers

Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk

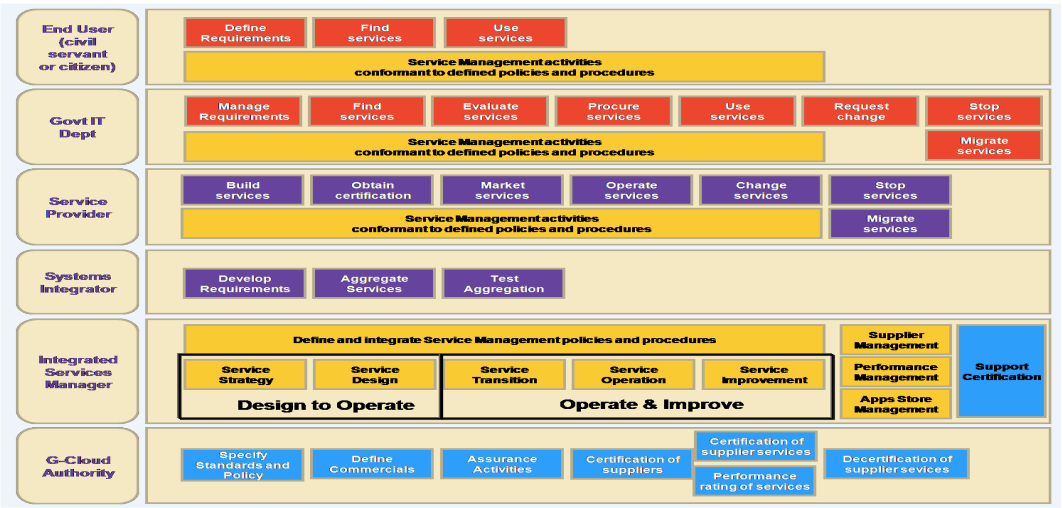
Assuring end to end service performance



Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk

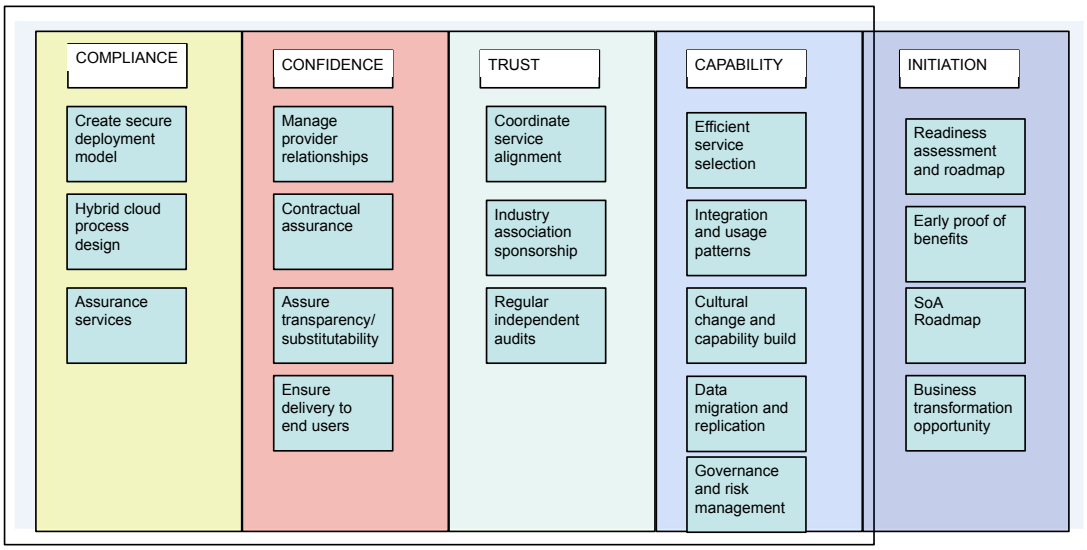
Assuring end to end service performance



Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk

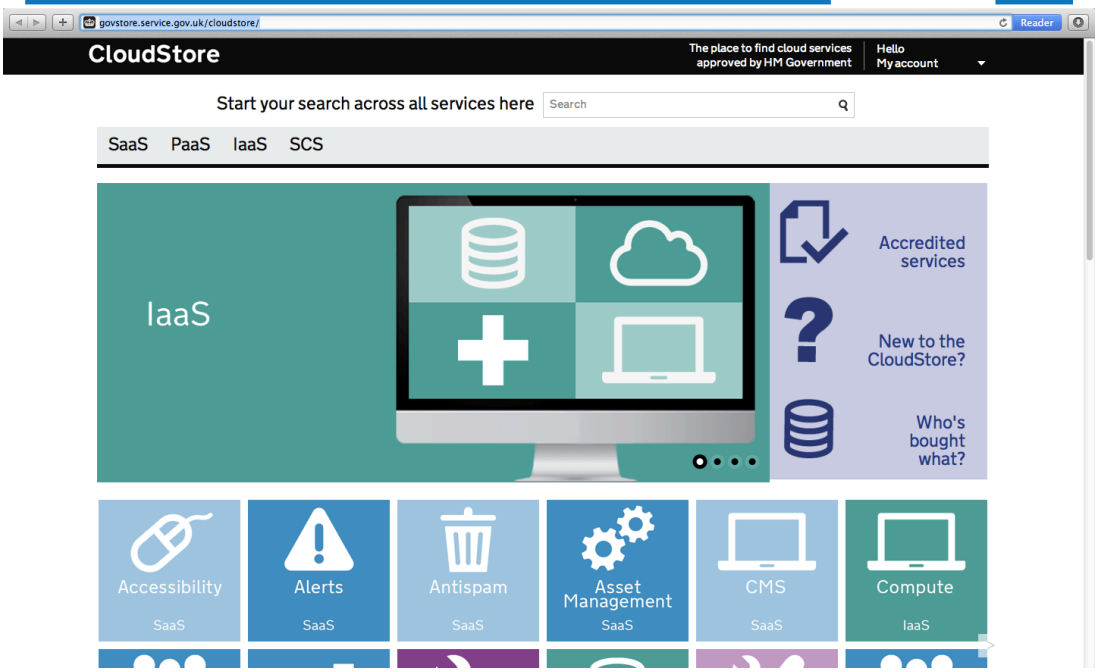
Cloud Services Brokerage Portfolio



Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk

http://govstore.service.gov.uk/cloudstore/



Martin Bellamy

Adoption of cloud computing services by public sector organisations

- The opportunity for cloud services brokerages to help overcome barriers to mainstream deployment -

Opportunity
When costs can be 80% lower why, in most large organisations, does cloud computing still account for less than 5% of the IT budget?

"Attractive in principle – difficult in practice"
-- organisations prioritise 'line of business' applications that are custom built, or configured, to reflect their unique business purpose.
-- cloud computing SaaS services do not immediately address organisations' unique business needs.
-- many needs can be addressed by using combinations of public cloud and internal services, but doing so robustly is costly.

Barriers to cloud deployment
Security
Design process
Operational management
Contractual concerns
Supplier management
Legal constraints
Resistance to change
Governance models
Standards

Solutions
Share the costs of addressing the challenges
via
Cloud Services Brokerages
Integrated Services Managers
Digital cloud marketplaces
Service Orientated Architectures



Establishing trust -- the critical success factor

"By March 2013, one year after launch, the UK Government CloudStore has 700 suppliers who have made 1,000 sales, with a combined value of £18 million"

Imperial College London

Martin Bellamy
Department of Computing, Imperial College, London, UK
m.bellamy09@imperial.ac.uk martinbellamy100@yahoo.co.uk