Government ICT Strategy

End User Device Programme

EUD Technical Framework Document – Phase 3

Protective Marking: Unclassified

(v1.1) – Part 1

PRODUCT CONTROL SHEET

Approved by		
Name	**Role**	**Date**
Phil Pavitt	Senior Responsible Owner /CIO	October 2012
Mark Hall	Deputy CIO	October 2012
Nigel Green	Programme Director	October 2012
	Programme Board Member (as appropriate)	
Authors		
Name	**Role**	**Date**
Steve Rowlands	EUD Programme Team	October 2012
Phil Reed	EUD Programme Team	October 2012
Phil Sharman	EUD Programme Team	October 2012
Kirsten Stewart	EUD Programme Team	October 2012

CHANGE HISTORY

Version No.	Date	Details of Changes included in Update
0.1	August 2012	Initial draft
0.2	August 2012	Revised after internal review
0.3	August 2012	Revised the structure
0.4	September 2012	Revised as per feedback from Steve R
0.5	September 2012	Revised the document as per review comments by Nigel and CESG
0.6	September 2012	Revised the draft as per feedback from Peer Review meeting
0.7	September 2012	Revised the draft as per feedback from EUD Programme Team
1.0	September 2012	Baselined version for release 3
1.1	October 2012	Final amendments for publication

DOCUMENT INFORMATION:

Master Location: EUD Programme Library

Table of Contents:

This document forms part 1 of the 3 part 'EUD Technical Framework Document Release 3'. It contains sections 1-5 which are referenced in Parts 2 and 3. Note that the appendix is contained in parts 2 and 3.

This version of the End User Device Technical Framework (Phase 3) sets out the detailed concepts and good practice associated with the End User Device Strategy (Cabinet Office, 2012).

Further work is being undertaken on identifying and defining the open and security standards for inclusion in the next version of the framework.

1 EXECUTIVE SUMMARY

This End User Device Technical Framework is a key component of the Government ICT EUD Strategy and presents a multi-tier reference architecture for devices. The vision for the End User Device (EUD) Strategy is to fundamentally redefine the range and role of end user devices within government.

Key strategic themes for renewed focus and change are:

1. End user devices which meet genuine **user needs**, and are convenient and efficient to use.
2. Greater **user choice** in the tools and services they need to do their work.
3. **A competitive market** for end user devices enabled by **interoperability standards**, with many more suppliers of all sizes, including **SMEs**, and no unjustified bias towards large or incumbent suppliers.
4. Increasing use of **consumer commodity IT** and **cloud services** where possible, minimising the overhead for bespoke and internal IT, and benefitting from consumer market value, innovation and user friendly services.
5. A level playing field for **open source** technologies, enabling lower costs and increased competition.
6. **Disaggregated** technical and service designs, combined with **shorter contracts**, enabling easier change of suppliers, improved cost transparency, reducing delivery risks from large bundled IT programmes, and avoiding conflict of interests for suppliers.
7. A drive towards **web based applications and services**, agnostic to any end user device type, vendor, operating system or browser.
8. Appropriate standards of **accessibility** and **sustainability** maintained.

The end user device market within government will be reinvigorated through greater supply-side competition driven by the establishment of this EUD Framework in conjunction with clear standards. These standards will include:

- **Interoperability Standards**: To be defined, these are likely to include open standards relating to virtual private networking, printing, authentication, consumption of web based services and remote virtualised applications.
- **Security Standards**: To be defined, these will be a clarification of controls for Tier 1 end user devices and associated services, within the context of the Government Protective Marking Scheme review. These are likely to include minimum standards covering areas such as encryption, platform and data integrity, device and user authentication, and requirements product assurance.

The EUD Strategy supports the Government's commitments in the **Civil Service Reform Plan**. It provides key improvements to the flexibility and usability of IT. The EUD Strategy is also a key enabler to the work within the Civil Service Reform Plan to promote greater flexible working and to pilot working from home IT solutions. This includes (Civil Service 2012, p.29):

- "Upgrading IT systems across departments to ensure they support flexible and efficient working methods.
- Updating IT equipment. With more streamlined security systems, there is greater scope to modernise the way in which the Civil Service contracts IT – a far wider range of devices, like laptops, can be procured much more cheaply, rather than requiring expensive, bespoke devices.
- Ensuring the security classifications of equipment matches the risks involved. A risk aware culture will be fostered across Government that understands the threats faced and what 'good enough' IT security looks like."

The recent annual report on the ICT Strategy published by the Cabinet Office (One Year on: Implementing the Government ICT Strategy) stated:

- "2.29 The Government published the EUD strategy in October 2011, which set out the aim that as far as possible, the public sector workforce will be able to work from any location on any suitable government or non-government end user device. Principles developed as part of the EUD strategy are now embedded into the next wave of central government procurement of EUDs, meaning that over time, government will converge on the model set out in the strategy.
- 2.30 Analysis of the data collated from the Quarterly Data Summary (QDS) reveals that there is significant variance on the cost of device per Full Time Equivalent (FTE), ratio of device per user, and boot-up time for devices across central government. The EUD programme has set a target of reducing the average cost of a device to a maximum of £500 per FTE with an average of one device per user. The programme will also aim towards an average boot-up time of 120 seconds (currently at 182 seconds). Over the next two to three years, departments will work towards these targets, but progress will depend on factors such as the contractual position (including termination options and costs) of departments."

DOCUMENT PURPOSE AND STRUCTURE

This interim version of The End User Device Technical Framework (Phase 3) sets out the detailed concepts and good practice associated with the End User Device Strategy (Cabinet Office, 2012). Further work is being undertaken on identifying and defining the open and security standards for inclusion in the full version of the framework. Whilst this interim version does not set out the complete EUD solution guidelines, it does present the emerging EUD multi-level reference architecture framework. The Level 1 and 2 Framework (Conceptual Framework) document can be found at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/End-User-Device-Programme-Conceptual-Framework-Release-1-4_0.pdf (Cabinet Office, 2012).

The EUD Technical Framework is divided into 3 parts:

Part 1 (this document) focuses on helping organisations make the right choices when adopting new end user devices. It outlines a simple 5 step process and includes an example scorecard to guide decision making.

Part 2 contains the detailed Solution and Implementation Guidelines based on the elements defined in the EUD Conceptual Framework. It highlights the characteristics and pros and cons of various options as well as best practices for implementation.

Part 3 maps the technical solutions identified in Part 2 on to each of the six identified EUD roles. It also includes detailed user scenarios to bring each solution to life through real world examples. It also contains individual case studies highlighting how organisations have implemented the solutions.

1.1 INTENDED AUDIENCE

The document is intended for the following audiences:

- Central and local Government organisations – Government organisations should use this document to guide their ICT project and procurement activities, to demonstrate that their overall technical approach is aligned to the EUD vision and all major changes are based on the EUD Technical Framework.
- Suppliers – Suppliers should use this document to ensure that any EUD-related services and solutions they propose are aligned to the EUD Technical Framework.

1.2 FRAMEWORK GUIDE INTRODUCTION

The End User Device (EUD) Framework presents a multi-level reference architecture. The purpose of the Framework is to:

- Identify the components that are in scope for EUD Strategy programme building on the Level 1 and 2 Framework.
- Provide a definition for each component within the Framework.
- Provide a mechanism, based on user roles, to identify best fit solutions and application technologies for each role.

1.3 Framework Lightboard Key

The Framework can be used to visually illustrate specific End User Device implementation combinations or scenarios. To illustrate this, key components within the framework are identified:

- **Highlighted Component** – Illustrates a component that is not only compatible with the scenario described but is also a ***recommended*** component. This is a solution that is best suited to the scenario.
- **Visible Components** – Illustrates a component that is ***compatible*** with the scenario described. The visible components show what is technically possible with the scenario.
- **Greyed Out Components** – Illustrates a component that is ***incompatible*** with the scenario described. These can be considered blocked routes. As such the component is not relevant for the presented scenario.

When the following patterns are applied to the Framework, the term 'Lightboard' is used.

FIGURE 1 – FRAMEWORK COMPONENT LIGHTBOARD KEY

2 MAKING THE RIGHT CHOICES

This section provides guidance to support government organisations in transforming their use of end user devices. It provides information on the steps to follow and identifies good practice to guide the transformation of devices and underlying environments.

The section will provide advice on a range of areas including:

- Decision making process
- Understanding the strategic business direction
- User segmentation
- Understanding the application estate
- Technology mapping to user segments
    - Choosing the right technologies
        - Introducing “Bring your own device”
    - Using Open Source technology
- Implementation
    - Use of virtualisation to provide existing applications during transition
    - Use of virtualisation to provide mobility across devices
    - Use of cloud based solutions or specialist software for file storage, collaboration, email
    - Creation of controlled zones between existing IL3 infrastructure and Tier 1 devices.

2.1 Decision Making Process

This section will help organisations to identify ways to use the framework and transform their end user devices or to validate their current model. The steps described here are aligned to the key strategic objectives set by government in its ICT Strategy document (http://www.cabinetoffice.gov.uk/sites/default/files/resources/govt-ict-sip.doc) and the objectives of the End User Device Strategy (http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-end-user-device-strategy_0.doc).

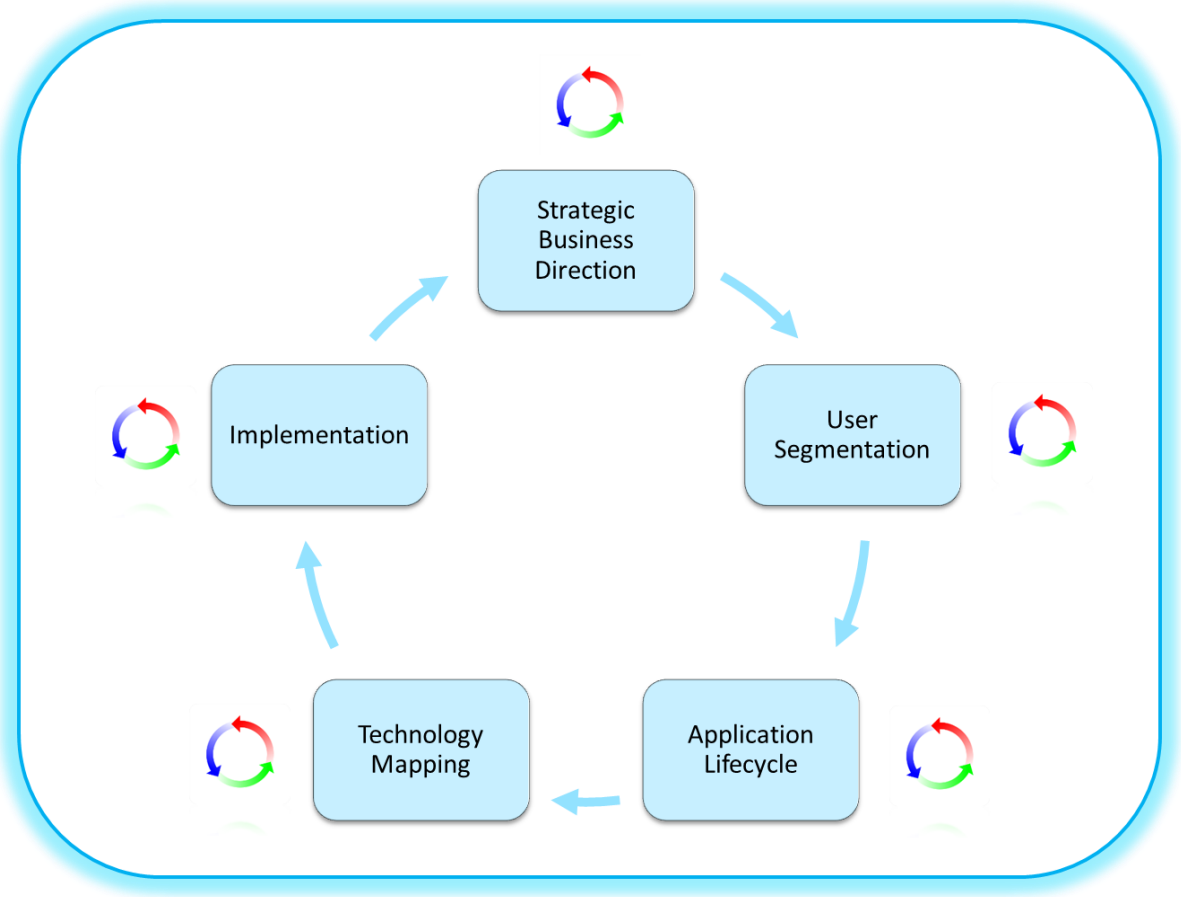

FIGURE 2: EUD TRANSFORMATION PROCESS

Organisations should adopt an iterative approach to the end user device transformation process described above; focusing on particular user profiles and requirements rather than the tradition 'one size fits all' approach. The principal steps to the process are:

1. The critical first step is to understand the strategic business direction, for example, a shift to new ways of working, which may influence the choice and selection of particular technological components.
2. Understand the users, their profile and their requirements. A detailed description of the EUD user profiles can be found in section 7 (part 3 of the document) and an example of how to segment users is available in section 3.3.

3. Understand and rationalise the core applications used by a particular user segment. A detailed description of the application life cycle is explained in section 3.4.
4. Select the technology that best serves a particular user segment or combination of user segments. The detailed explanation of available technologies to achieve this is provided in section 6.1 (Solution Guidelines) - part 2 of this document. This section will also guide through the best combinations of devices and components.
5. The final step is to identify the changes required to the underlying infrastructure and environment to support the transformation and rollout of devices to users. This is detailed in Section 6.2 (Implementation Guidelines) – part 2 of this document. Implementation (including security accreditation) of new devices and the supporting infrastructure will be the responsibility of individual departments as will delivery of the realisable benefits.

2.2 Strategic Business Direction

Before embarking on an end user device transformation programme, an organisation should ensure there is a clear view of its strategic business direction. A key focus of Government's ICT Strategy is increasing the productivity, flexibility and mobility of the workforce, allowing government organisations to be more agile and deliver better value at lower cost. The strategy also includes government's commitment in other areas, such as Green policy, the use of Open Source software and Open standards. More details about the overall strategy can be found at:

http://www.cabinetoffice.gov.uk/sites/default/files/resources/govt-ict-sip.doc

http://www.cabinetoffice.gov.uk/content/government-ict-strategy-strategic-implementation-plan.

Other important considerations include:

- The organisation's plans to implement Civil Service Reform.
- The need to demonstrate compliance with government security policy.
- The organisation's risk appetite and overall approach to information risk management.
- The organisation's policy on Bring Your Own Device (BYOD).
- The government's ICT Strategy including strategic goals for open source, open standards, cloud services, SME suppliers, use of consumer commodity IT, and disaggregation of technology and commercial designs.
- HR strategy and policies on home working, mobile working, flexible hours etc.
- Future plans for estates management and consolidation.
- Legislation and regulatory controls.
- Other related organisational policies such as hot-desking, outsourcing, service management.

The EUD framework presents a multi-tier reference architecture for devices and aims to de-couple the various components, for example the operating system and the end-user applications, from the underlying endpoint or device. The Vision Statement for the End User Device Programme sets out the following goals relevant to this document:

- Deliver a set of guidelines and standards (to include characteristics and definitions) for devices and their use within government, taking into account service management and security requirements.
- Wherever possible, public sector workers should be able to access the services they need to carry out their job from any location, on any suitable government or non-government end user device.
- Implementation (including security accreditation) of new devices, software's and the supporting infrastructure will be the responsibility of individual departments as will delivery of the realisable benefits. Departments will be required to demonstrate that their overall technical approach is aligned to the vision and all major changes to devices are based on the new architectures and standards. Before the departments do this, they should ensure that they have the appropriate business case to implement particular technology solutions and identified the business change process and the Total Cost of Ownership (TCOs) involved.

2.3 User Segmentation

User Segmentation is a process of defining categories of employees based on how they use IT as part of their day to day job. Users in the same segment share similar characteristics so that recommended technology solutions can be tailored to their specific needs and requirements.

The goal of segmenting the user population is to provide users with better solutions matched to their computing needs while providing increased capabilities at lower costs to Government. Typically, most large organisations have between 4 and 6 user segment types. The challenge when segmenting users is to avoid becoming too granular and rendering the exercise too difficult to manage and support. User Segmentation is explained in detail in levels 1 and 2 of the Conceptual level framework (which can be found at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/End-User-Device-Programme-Conceptual-Framework-Release-1-4_0.pdf) and six main user profiles have been identified (see Table 1).

User Profiles	Characteristics
Line of Business user	Typically performs a small number of dedicated processing tasks from a trusted location. For example, users who work in a contact centre or back office processing role such as PAYE. They use Line of Business applications, which serve a specialist customer transaction or business need.
Mobile Knowledge user	Typically uses generic productivity tools e.g. email, word-processing, internet access to perform core activities on the move (including working without network connectivity). They have little or no reliance on Line of Business applications.
Knowledge User	Primarily use rich productivity tools e.g. email and word-processing to perform core activities. Unlike mobile knowledge workers, they work from a fixed office location. Examples of knowledge workers might include policy workers, managers and others.
Hybrid User (Line of Business / Knowledge User)	Balance their IT usage between Line of Business systems and creating documents or manipulating data with productivity tools, from a fixed location or locations (commonly an office or offices). These might be caseworkers, line of business managers etc.
Field User	A Field user needs access to Line of Business and productivity applications, which are available on the move (including offline). A Field user might be a visiting officer, investigator or caseworker who needs to access or update customer records both online and offline as well as create documents and manipulate data.

Occasional User	Occasional Users have no reliance on IT to complete their core activities and only need access to systems to carryout supporting tasks such as viewing their payslip or booking annual leave. These tasks could be carried out on a device shared with other users in the category.

TABLE 1 – USER PROFILES

Most of the user population should fall into one of these categories. When an organisation starts the process of user segmentation, it is important to understand the user profiles identified in the Conceptual level framework before classifying their user population accordingly. A table like the one above can be used to capture the approximate percentage of users that fall within a particular user profile. In some cases, it may be advantageous to break down each profile into further sub-categories of users. However, care should be taken to avoid creating too many sub-categories within a particular user profile. Government organisations should consider creating a new user profile only under exceptional circumstances, when a particular user group cannot be fit into any of the user profiles identified in Table 1.

2.4 APPLICATION LIFECYCLE

A key element to desktop transformation is the process of identifying, categorising, and rationalising applications in the current desktop application estate. Identifying and understanding the applications used within an organisation forms the basis for mapping technology and end user devices to a particular user profile.

It is important to understand the governance, development and maintenance processes for an application. Key points to consider are:

1. What business requirements does the application support?
2. What's the usage profile for this application? For example:
    a. How many users access the application?
    b. How long do they access it for?
3. Has a baseline security configuration been agreed, documented and applied – is it transferable?
4. How does the application operate?
5. Is the application dependent on any hardware or software components?
6. What are the hardware and network requirements for optimal running of the application?
7. Which environments can the application be run in? E.g. Virtualised.
8. How do users access the application?
9. Is the application owned/supported externally or internally?
10. Is the application covered by a support contract that specifies any connectivity/device requirements?
11. Costs – licence renewal, specialist training for users, maintaining associated software modules etc.
12. Is it off the shelf or bespoke?
13. Is it a legacy application (if so its continued use needs careful consideration to prevent further embedding?)
14. What is the business impact from a loss of availability?
15. What is the application 'shelf life' - when will it be replaced or vendor support withdrawn for this version?
16. Are there better value and more strategically aligned alternatives to the application which would justify investment to change?
17. Does the application create a dependency on a single supplier's desktop or operating system, and can this be remedied?
18. Other factors such as security, business ownership and service criticality of the application.

Answers to these questions will define whether a particular application can be packaged and presented to the user in a different, more cost effective way. The answers will also define what technology components are available for delivering and interacting with the application and what end user devices are compatible for presenting the application to the users.

This section will guide organisations in transforming their desktop application estate. During this transformation, organisations should rationalise their applications, removing applications that are no longer required or have limited use for a disproportionate cost.

Key activities in planning for an IT Transformation Journey are:

- Understanding your business and establishing an environment that strikes a balance between business opportunity and risk.
- Understanding your existing desktop application estate.
- Application rationalisation.
- Identifying the most appropriate target platforms for applications.
- Making applications available on these new platforms.

As a journey planning aid, a desktop application lifecycle is presented below.

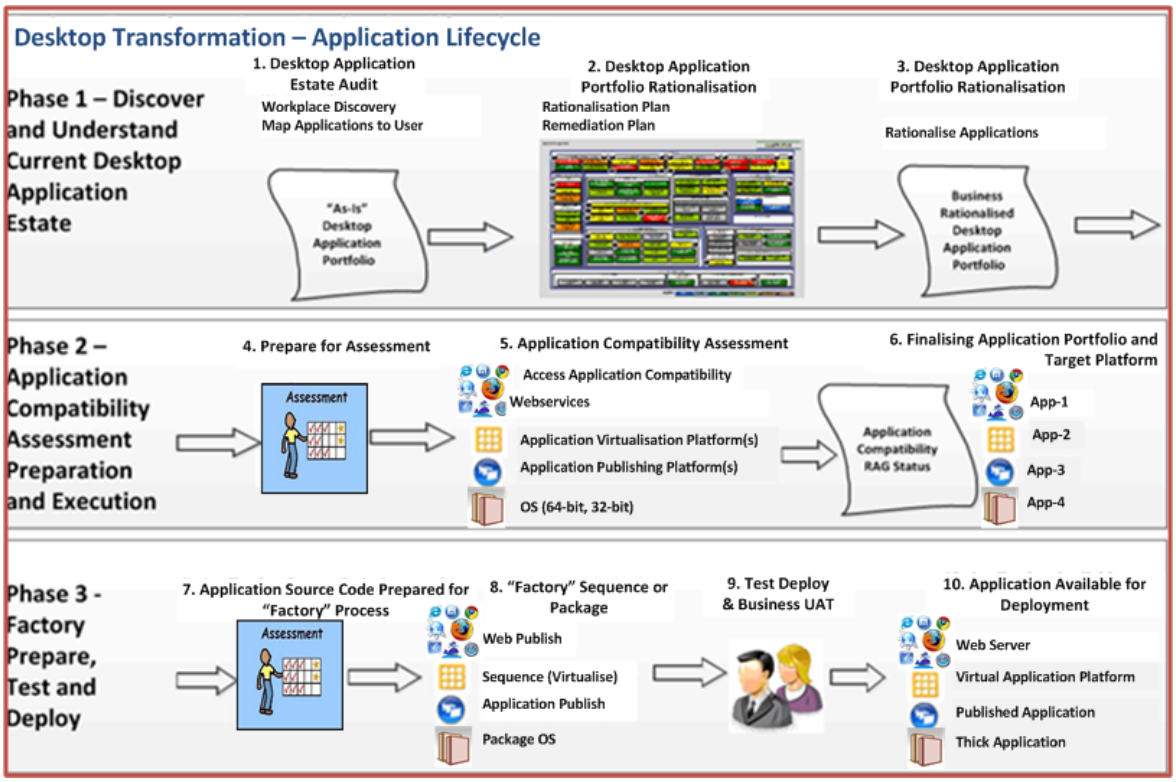

FIGURE 3: APPLICATION LIFECYCLE

This diagram depicts the common lifecycle for applications. If an application cannot be simply migrated, then it may need to be upgraded, re-written (if appropriate), replaced or switched to a web based version of the application.

In line with the diagram above the key phases of the application lifecycle are:

2.4.1 Phase 1 - Discover and Understand Current Application Estate

Discovery of the 'As-Is' application estate is the key first stage of the Desktop Application Lifecycle. This is a planning phase.

The key stages are:

- **Desktop Application Estate Audit** – Firstly the existing application estate needs to be analysed. This establishes the desktop applications currently available to the organisation's user base. This activity should ideally involve technical input (i.e. using application discovery tools in the environment to establish installed applications) and also business input (e.g. interviews with business areas to understand the applications critical to the organisation). The outputs of this activity are an "As-Is" Application Portfolio.
- **Desktop Application Portfolio Rationalisation –** the "As-Is" Application Portfolio is reviewed, identifying any applications suitable for retirement or replacement, and standardising on applications where multiple versions share similar functionality. Many government organisations will have a wide variety of "business developed applications" often built around adding functionality through macros or Visual Basic for Applications (VBA) extensions to Microsoft Office. Without rationalisation these are likely to be a blocker to adopting different technology solutions.

The output from this stage is a "Business Rationalised Application Portfolio" and is focused on reducing overall estate cost.

2.4.2 Phase 2 – Application Compatibility Assessment, Preparation and Execution

This phase focuses on comparing applications with target architectures, with a view to identifying compatible solutions and the lowest cost platforms on which applications can be delivered.

Figure 4 offers a generally accepted industry view of the relative cost and complexity (in terms of difficulty of implementation and maintenance) of different application delivery platforms.

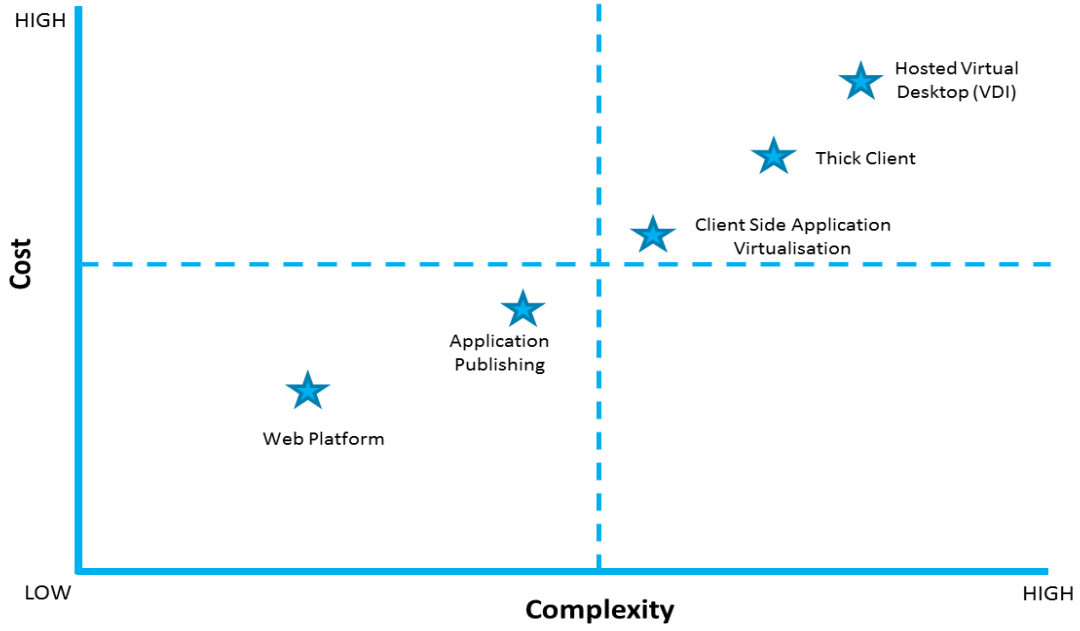

FIGURE 4 – DELIVERY PLATFORMS AND TECHNOLOGIES

Important Note

Factors like the size of an organisation, the number of applications it has and the complexity involved in remediating them can have an impact on the cost & complexity of particular application delivery platforms.

Typically the applications within an organisation will fall into the following categories:

- **Web based applications -** some may have been written to exploit features of older versions of a web browser (often IE6) and should be assessed for compatibility with web standards (HTML-5). As the application typically runs on a backend server no other application changes are required.
- **Thick applications** – some applications will run without amendment on a different operating system and simply require some degree of testing. But note that any decision to use an application on a different platform or expose it to a different connectivity path should be considered by a risk assessment. Assurance should also be sought to ensure the application is secure (also think about security accreditation, security policy updates and baseline security configuration).
- **Virtualised applications** – can be an effective way of packaging applications to run in a sandbox client on the desktop avoiding changes to system files or registry and avoiding conflicts with other applications.
- **Applications that need remediation** - many applications in government will be written to run on legacy Operating Systems and will require changes to ensure compatibility with the target platform. An alternative is to implement a server based computing solution using hosted desktop environments.

Compatibility with the above platforms could theoretically be done manually by discussion with application vendors. However, unless the number of applications is very small, use of an Application Compatibility Assessment Toolset is recommended. There are a number of vendors who provide Application Compatibility Assessment Toolsets. Commonalities between applications should be noted as these may inform decisions of the presentation method chosen, for example multiple applications may be accessible through the browser.

The three stages of this phase are:

- **Prepare for Assessment** – Gather the information required for the Application Compatibility Assessment Toolsets.
- **Application Compatibility Assessment**- Applications are typically processed in batch mode, producing a RAG status report indicating each application's compatibility with the target application platforms. Green applications can generally be easily remediated to work on the platform, with Yellow indicating increasing levels of remediation and Red indicating an underlying compatibility issue (i.e. the application cannot be made to work on the given platform).

- **Finalise Application Portfolio and Target platforms** - The primary objective of this stage is to identify and document the target platforms on which each application will be delivered, based upon the information in the report. Decisions may also be made to retire additional applications (i.e. applications incompatible with the target platforms).

2.4.3 Phase 3 – Factory Prepare, Test and Deploy

This phase of work is undertaken during implementation, and involves preparing applications for delivery to the target platforms (typically called sequencing for virtual applications, packaging for thick client applications and publishing for web and published applications). The term 'Factory' is used, as for a large organisation it is recommended that standards for the application sequences or packages are put in place and an industrialised process used. Many suppliers offer an 'Application Factory' service, and this typically involves an organisation engaging a supplier to prepare their applications for a new platform, often paying for the service on a per application basis.

The four stages of this phase are:

- **Application Source Code Preparation for "Factory" Process –** Application publishing, sequencing and packaging require the application source code to be made available. At this stage the application source components and associated information are gathered.

- **"Factory" Sequence or Package –** The application is prepared for the target platform – published, sequenced or packaged. If an application cannot run in the new environment, it should be assessed whether it should be replaced. Alternatively, the applications can be run using a "sandbox" approach. This could be done using a virtual machine running side by side on a powerful PC, or hosted in a datacentre where it is managed centrally and used by multiple users.

- **Test Deploy and Business UAT (User Acceptance Testing)** – Applications are tested by the business to ensure that they work correctly on each platform. Typically this involves a testing key functionality and signing off with the user ready for deployment. Applications that fail the UAT process are returned to the "Factory" process for further remediation. Appropriate security assurance procedure should be in place to ensure that the code does not contain malicious functionality.

- **Application Available for Deployment** – This marks the end of the process.

2.4.4 Considerations for Locally Developed Applications

The following are key considerations in handling locally developed applications (macros etc.) when changing the desktop environment:

- What is the business requirement?
- Confirm the organisation's policy towards locally developed applications and any standards and governance that may be introduced to manage such applications.
- Identify an owner for each application.
- Identify all the applications that are used locally.

- Identify if any applications contain assets which could be extracted.
- Rationalise to identify the applications for retirement, replacement or standardisation (for those providing similar functionality).
- Identify if the applications can be moved onto the new environment and if they can maintain the same standards as before.
- Identify any issues that may arise during migration to the new environment.
- If an application cannot run in the new environment, it should be assessed whether it is cost efficient to be re-written or requires a virtual desktop implementation.

2.5 Technology Mapping to User Segments

Mapping technology to user segments is the process of evaluating technologies and devices, against defined selection criteria to find the best fit for each user segment; this allows government to provide the right technology solution per segment, ensuring the proper balance of IT capability with end-user needs.

Section 6.1 (part 2) of this Framework provides list of technologies that are currently available in the market place and have been identified as a best fit for a particular user profile. There may be exceptional cases where the technology identified is not adequate for a particular usage scenario or newly identified user segment. In such cases, technology outside the EUD Framework might be considered if supported by a strong business case. This section outlines how this mapping could be carried out in a particular government department or organisation.

The technology mapping process provides a method by which tailored solutions can be managed and re-evaluated in a logical and methodical way. Providing one solution across all user roles will not deliver the right computing power to the right people. Similarly, providing unlimited, unique computing solutions for all users will be cost prohibitive and unmanageable. Therefore, establishing a model where each user segment is assigned an optimal technology solution enables government to have a simple and cost effective method to match the right devices to the right people.

It is essential to evaluate technologies in a systematic way. The evaluation criteria rankings should be influenced by business requirements as well as IT readiness. Technologies should then be compared against each other on a segment by segment basis to produce an optimal mix of technology solutions.

The approach may vary dependent upon the procurement vehicle to be used, such as an OJEU procurement, Government Procurement Service Framework or dynamic procurement (such as G-Cloud). An example of the process that can be used to map technology to user segments is described in the following sections.

2.5.1 Step 1: Choose The Technologies That Are Applicable To Your Work Environment

It is important to identify the range of devices that are being considered for different user profiles within the organisation. These might include:

- Desktop
- Thin Client
- Laptop
- Smartphone
- Tablet

Details of all device types can be found in section 6.1.5.2 (part 2 of this Framework).

To help guide the selection process for devices and technological components, a scorecard approach can be used. To compare two or more competing solutions, scores can be given based on a series of

given factors and factor weightings. The total scores for each solution then indicate the fit of that with the priorities of the organisation. An example scorecard can be found in section 3.5.3.

2.5.1.1 Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) can be defined as a business policy of employees bringing personally owned mobile devices to their place of work and using those devices to access privileged company resources such as email, file servers and databases as well as their personal applications and data. BYOD allows users to work on their device of choice, which can increase employee satisfaction and also lower IT costs to the enterprise. There are however, recognised risks to BYOD – see below.

The trend for IT consumerisation is driven by a number of factors. While smartphone and tablet usage is on the increase globally, employees often find that their personally owned devices are better and more reliable than those provided by their organisations. Given that device refresh programmes are notoriously expensive, it may not be surprising that many workplaces have failed to keep up with the fast pace of technological advances in the consumer market. A BYOD strategy therefore represents an opportunity to leverage employees own devices and has potential to reduce costs for the organisation.

Whilst BYOD is not likely to replace main stream provisioning of devices in all user roles across government, it does provide some opportunities to increase user satisfaction and reduce cost. For the most part it is likely BYOD would provide only a secondary or tertiary device. However, some Mobile Knowledge users with official laptops for example may prefer to become standard knowledge workers by using cheaper thin desktops at office locations. They could then use their own devices in a controlled manner at home or on the move. It is important that organisations understand and assess the specific security risks with the introduction of BYOD. The CESG Information Assurance Note 2012/07 (BYOD: The Risks from Personal Devices) explores these risks and provides guidance on a potential risk management approach.

It is also important that organisations understand the other factors which should be considered when gathering a complete perspective on BYOD, for example the tax implications.

The figure below provides a high level comparison between a traditional enterprise approach and a consumerised device model:

Attribute	Traditional Device Approach	BYOD Approach
Choice	Users have little or no choice of devices.	Users are able to select the device of their choice, within constraints set by their organisation.
Support	Device is fully managed and supported by the enterprise giving guaranteed service levels and resolution of issues and problem	User takes responsibility for supporting and maintaining the device. IT department typically provides standards and guidance for connection to corporate networks and high level support for business applications.
Cost	Costly for IT department. No cost impact	Cheaper initially for IT department as the

	to end user.	user is responsible for costs of own device including its warranty and insurance, but the future maintenance costs may increase.
Lost/Stolen Devices	Lost or stolen devices are replaced at a cost to the organisation.	Users are responsible for replacing own devices if they are lost or stolen, but organisations may try to enforce an agreement with users to ensure the device is replaced in a timely manner.
Security	The device is managed and secured in line with organisational policies which often restrict functionality or use e.g. access to social networking sites.	Information will not be as secure as on a device exclusively controlled by the organisation. Increased risks of compromise or loss which will need to be assessed and managed.
Ownership	The organisation owns the device and it must be returned when a user leaves.	The employee owns the device and bears the cost of upgrade or replacement.

TABLE 2 – BYOD VS TRADITIONAL DEVICE APPROACH

More details about the benefits of BYOD and key considerations on policies, adoption etc., can be found in Section 6.9.

2.5.2 Step 2: Evaluate The IT Landscape For Technology And Process Readiness

After an initial range of devices have been identified, the current IT landscape should be evaluated against the information and key attributes set out in sections 6.1-6.5 (part 2 of this Framework) and the further information in this section, to assess the viability of implementing these new technologies.

2.5.3 Step 3: Complete Device Scorecards For Each Technology Per Segment

A scorecard should be constructed to aid the process of evaluating different technologies. Scorecards are designed to calculate a score based on weighted, evaluation factors which should be carefully selected to provide a rounded approach in the assessment of each device. The evaluation factors and weightings should produce a balanced, final score.

Each device should be scored within context of each user segment. This will result in differing scores for the same device in different segments. Devices and technologies with close scores may be recommended as a complementary or optional solution for a user segment. Listed below are some evaluation factors, which can be used in this analysis:

Evaluation Factor:	Description:
Price	What is the cost of the device?
Maintenance Cost	What is the cost to service or replace the device?
Scalability	To what extent is the solution scalable or upgradeable?

Availability	Is it there when users need it?
Reliability	Could the solution negatively impact productivity due to unavailability or failure?
Performance	How fast is the technology perceived to be (response and boot up times)?
Level of Change	How well will users adopt the technology?
Training Requirement	How much training and documentation will users need?
End-User Expandability	Can the device handle extra memory, storage etc, to extend its life?
Maturity	Have other organisations implemented this solution (reference sites)?
Multi-vendor Solutions	Supported by major hardware / software vendors?
Security	Does this device meet the government Identity Assurance requirements set out by CESG and any requirements for connection to PSN and/or Gcloud services?
Mobility	How effective on a train, in a hotel or coffee shop, in another office?
Power Consumption	Significant?
Data Integrity	How is local data protected and backed up?
Future Viability	Is the market share growing or declining?
Peripheral Support	Does this device support USB or other peripherals?
3D Graphics Support	Can the device display intensive graphics?
Government Readiness:	
Applications	Is the Government infrastructure compatible with applications on this device?
Network	Does the network support the technology?
Hosting	Does the data centre support the technology?
Support Infrastructure	Do the support staff have the required knowledge, 3rd party contracts, and tools?

TABLE 3 – DEVICE EVALUATION FACTORS

By weighting evaluation factors according to organisational priorities, the scorecard will identify appropriate devices and technologies. Below is an example of a completed Technology Scorecard:

Technology Evaluation Scorecard

Total Score:	103

How to use this scorecard: *This scorecard allows relative comparison of two or more technology solutions for a set of users with similar roles:*
1. For the set of users being considered, fill in the 'Weight' column, indicating the relative importance of each factor for that group of users. Weights should be entered so that their total equals 100%.
2. For each solution being considered create a copy of this sheet and fill in the 'Score' column using the scale below and entering comments where necessary.
3. Compare the total scores for each solution, a higher score indicating better alignment of a solution with the needs of the user group being considered.

Segment:	Line of Business User
Technology Name:	Thin Client with SBC
Definitions:	SBC - A Server Based Computing (SBC) Receiver is the client side component of Server Based Computing delivery methods (e.g. Application Publishing and Hosted Virtual Desktop). The client side component, installed on endpoint device to receive a data stream from the server based

Scale		
Unfavorable	Average	Favorable
0 1 2 3 4	5 6 7 8	9 10

Evolution Factor	Description	Score (1-10)	Weight (%)	Weighted Score	Comments
The Solution					
Price	Cost of solution	3	17%	5.0	Initial cost isn't favourable but this should be off set by other benefits
Maintenance Cost	Cost to service or replace the solution	6	17%	10.0	
Scalability	How well will this grow?	9	4%	3.6	
Availability	Is it there when users need it?	7	6%	4.4	
Reliability	Will it negatively impact productivity due to failure?	7	6%	4.4	
Performance	How fast is the technology perceived to be?	4	4%	1.6	
Level of Change	How well will users adopt to technology?	8	4%	3.2	LoB applications used should have no discernible change to the end user
Training Requirement	How much training and documentation will users need?	8	2%	1.6	
End-User Expandability	Can the soultion handle e.g. extra memory, storage or speed?	7	2%	1.7	Easy to upgrade in this manner from central location
Maturity	Are there organisations who have been using this for more than a year?	7	6%	3.9	
Multi-Vendor Solution	Do the major HW/SW vendors support this?	8	3%	2.5	
Security	How is data protected?	6	8%	4.8	
Mobility	How can people work away from their desk?	1	0%	0.0	
Power Consumption	How much electricity is required for the device?	5	2%	1.2	
Data Integrity	How is local data protected and backed up?	7	8%	5.6	
Future Viability	Is the market share growing or declining?	9	4%	3.6	
Peripheral Support	Does the solution support USB or other peripherals?	2	1%	0.2	
3D Graphic Support	Can the device display intensive graphics?	3	1%	0.2	
Support for Open Stand	Does the device / technology support major open standards	7	4%	2.8	
Accessibility Support	Support for impaired users	6	1%	0.6	
Offline working	Can the solution work with no network connection to datacenter	0	0%	0.0	
			100%		

FIGURE 5 – EXAMPLE TECHNOLOGY EVALUATION SCORECARD

An example scorecard is embedded opposite.

Scorecard.xls

The technology mapping process represents the synthesis of a number of different outputs, including the user segmentation and the organisation's choice of specific technologies and devices. The scorecards produced by this exercise can provide guidance in shaping the technology recommendations and as an input to a Technology Mapping Workshop.

2.5.4 Step 4: Conduct a Technology Mapping Workshop

The purpose of the Technology Mapping Workshop is to collaboratively reach a consensus regarding the devices and technologies applicable to each user segment and finalise a recommendation.

The participants of this workshop should include a range of stakeholders, including representatives from the End User Device team, and other impacted areas of the organisation, which may include the Architecture team, and the Technical Services team.

Technology mapping is a process of aligning technology with business goals. Section 6.1 (part 2 of the document) provides detailed information on a range of technologies that could be combined to allow users to connect to their corporate networks and access information to help them to perform their daily tasks. The key technologies discussed here are around:

- Traditional Desktop Infrastructure
- Server Based Computing

    - Desktop and Application Publishing or Shared Remote Desktops
    - Hosted Virtual Desktops or Virtual Desktop Infrastructure (VDI)
- Web Enabled Application Access
- Application Delivery Method
    - Cloud based
    - Traditional
    - Mix of both scenarios
- Enterprise Security

2.5.5 USING OPEN SOURCE TECHNOLOGY

Levelling the playing field for open source technologies is one of the key elements of the Government's ICT strategy programme (Cabinet Office, 2012). This means overcoming historical barriers to a genuine evaluation of open source technologies, including myths around security and support, unintended bias through procurement processes, and a lack of customer-side knowledge and experience of open source.

Open source can provide significantly lower total cost of ownership, conformance to open standards, and competition to otherwise complacent markets. Open source technologies have proven themselves in large, business critical or high security deployments across many sectors, including in government.

Further guidance and support can be found at the Cabinet Office Toolkit at:

http://www.cabinetoffice.gov.uk/resource-library/open-source-procurement-toolkit

For clarity, there are good and bad technology choices possible with both open and proprietary technologies. The strategy and policy promote aims to ensure good value technology and solution options are not missed.

A starting point for open source suggestions can be found within the Toolkit:

http://www.cabinetoffice.gov.uk/sites/default/files/resources/Open_Source_Options_v2_0.pdf

2.6 IMPLEMENTATION

This section provides implementation guidance and discusses some of the changes to an organisation's underlying infrastructure and environment to support the transformation of End User Devices. The key focus areas here include:

1) Use of virtualisation to provide existing applications during transition.
    a. To open up the desktop, organisations must ensure that they separate the applications and services from the individual devices. The use of virtualisation techniques can be an effective tool to achieve this separation. The use of desktop and/or application virtualisation can be a useful mechanism for managing existing applications during and after transformation.

2) Use of virtualisation to provide mobility across devices.
    a. The use of virtualisation techniques also provide users with the ability to access the same applications from a number of different devices and maintain consistency and persistence. There are sometimes limitations on the user experience when compared with applications that are native to a device. However, the benefits of mobility and flexibility may outweigh such limitations. Application virtualisation using Server Based Computing has been discussed in detail in Section 6.1.1 (part 2 of this Framework).

3) Use of cloud based solutions or specialist software for file storage, collaboration, email.
    a. The use of cloud based solutions can provide an effective way to introduce new services which can support and enable improved flexibility and mobility as well as contributing to the separation to devices from the applications and services which use them. Services such as those offered on the Government CloudStore provide organisations with the ability to move some of their corporate applications into the cloud. The nature and design of Cloud based services makes it easier to provide across a range of devices and locations. Strong candidates for consideration are collaboration, file sharing, email and office productivity applications.
    b. More details about Government's cloud strategy including benefits, managing risks/issues, delivery and implementation can be found at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.doc

4) Creation of controlled zones between an organisation's core infrastructure and Tier 1 devices.
    a. The Government Protective Marking Scheme review creates the opportunity for organisations to consider how they want to enable increase mobility and flexibility whilst maintaining the appropriate security. Organisations should consider creating a controlled zone, with the relevant technologies and security procedures in place to facilitate the connection of trusted and potentially untrusted Tier 1 devices to their infrastructure. Organisations should consider the good practice guides, policies and guidance issued by CESG

As discussed in Section 3.1, organisations should adopt an iterative approach to the end user device transformation process. The rollout should be carried out in phases, with a pilot phase carried out before the mass rollout of the solution. A pilot rollout provides an opportunity to test the various components of the solution within a small user community, and resolve any outstanding issues. It is important to collect the feedback from the pilot, as it can be used to improve training and end user support during future rollouts. The next stage after the pilot rollout is to ramp up and deploy the solution to each business unit on an iterative basis. The following diagram provides some insight into implementation planning.

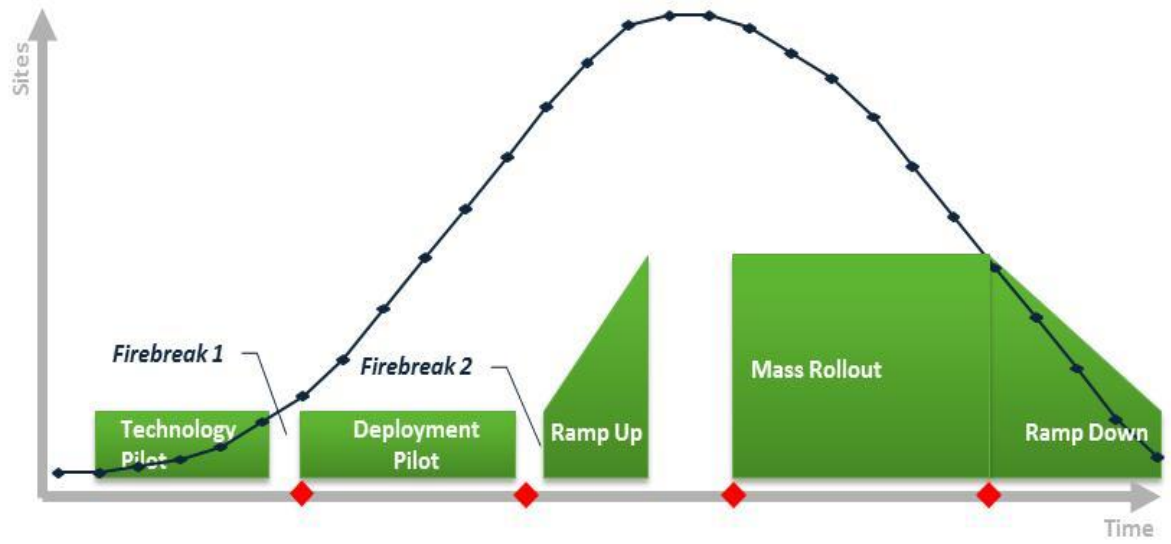

FIGURE 6 - IMPLEMENTATION PLAN

At each stage of rollout, there should be regular checkpoints to measure the overall effectiveness of the deployment and the key learning's and feedback should be captured to improve the process.

3 REFERENCES

The following documents are referenced in this document:

Reference	Date
BASSO, M. and TRONI, F. 2012. Segmenting Users for Mobile and Client Computing (Document # G00227122). *Gartner*.	February 2012
BBC. 2006. BBC's Future Media Standards and Guidelines. Available at: http://www.bbc.co.uk/guidelines/futuremedia/accessibility/	Accessed: 31st May 2012
Cabinet Office. 2012. End User Device Strategy. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/End-User-Device-Programme-Conceptual-Framework-Release-1-4_0.pdf	March 2011
Cabinet Office. 2012. EUD Conceptual Framework (v1.0).	March 2012
Cabinet Office. 2012. PSN Cyber. Operation Security Architecture.	April 2012
Cabinet Office. 2012. Open Source Options for Open Source.	April 2012
Cabinet Office. 2012. All About Open Source.	April 2012
Cabinet Office. 2011. Open Source Procurement Toolkit. Available at: http://www.cabinetoffice.gov.uk/resource-library/open-source-procurement-toolkit	Accessed: 22nd June 2012
CESG. 2012. Policy and Guidance. Available at: http://www.cesg.gov.uk/PolicyGuidance/Pages/index.aspx	Accessed: 22nd June 2012
CESG. 2012 Secure By Default: Platforms.	May 2012
Civil Service. 2012. Civil Service Statistics. Available at: http://www.civilservice.gov.uk/about/facts/statistics	Accessed 19th June 2012
Civil Service. 2012. The Civil Service Reform Plan. Available at: http://www.civilservice.gov.uk/wp-content/uploads/2012/06/Civil-Service-Reform-Plan-acc-final.pdf	Accessed 31st August 2012
COSGROVE, T. 2012. Magic Quadrant for Client Management Tools (Document G00225953). *Gartner*.	January 2012. Revised February 2012.
CROOK, S, T., DRAKE, S,T., STOFEGA, W., and LLAMAS, R, T. 2011. Worldwide Business Use Smartphone Business Use Smartphone 2011-2015 Forecast and Analysis, Volume 1 (Document IDC #230311). *IDC*.	September 2011

DirectGov. 2010. Disability and Equity Act 2010. http://www.direct.gov.uk/en/DisabledPeople/RightsAndObligations/DisabilityRights/DG_4001068	Accessed: 14th June 2012
Europa. 2011. WAI – WCAG 2.0. http://ec.europa.eu/ipg/standards/accessibility/wcag-20/standard_wcag_en.htm	Accessed: 06 July 2012
ENTERPRISEIOS. 2012. Comparison of MDM Providers. Available at: http://www.enterpriseios.com/wiki/Comparison_MDM_Providers	Accessed: 1st June 2012
Equality and Human Rights Commission's (EHRC), Disability Discrimination Act, Guidance on matters to be taken into account in determining questions relating to the definition of disability. Available at: http://www.equalityhumanrights.com/uploaded_files/guidance_on_matters_to_be_taken_into_account_in_determining_questions_relating_to_the_definition_of_disability.pdf	Accessed: 14th June 2012
EUD Component Definition and RACI MATRIX	February 2012
GIRARD, JOHN and OUELLET, ERIC.2011. Magic Quadrant For Mobile Data Protection, September 2011 (Document # G00215848). *Gartner*.	September 2011
HOCHMUTH, PHIL. 2011. World wide Data Loss Prevention 2011 – 2015 Forecast and 2010 Vendor Shares: DLP Gets More Embedded into Enterprise Infrastructure, Volume 1 (Document # 231367). *IDC*.	December 2011
IDC and Kensigton® "Your Laptop, Your Responsibility" A Suggested Physical Laptop Security Policy for Private and Public Organisations by Kensington and IDC (Document # IDCVP06R). *IDC.*	2009
JOHN GIRARD, JOHN PESCATORE and TIM ZIMMERMAN. 2011. MarketScope for Wireless LAN Intrusion Prevention System (Document # G00213850). *Gartner*.	July 2011
JOHNSTON TURNER, M. 2012. World Wide Change and Configuration Management Software 2011 Vendor Shares, (Document # IDC235073). *IDC*.	May 2012
Lambert, N. and Herald, A. 2009. Bring Your Own PC Reinvents The Corporate PC: A Citrix Systems Case Study. *Forrester*.	2009
MACGILLIVRAY, C. 2011. Tablets in the Enterprise: Opportunities and Challenges for Businesses and Mobile Operators, Volume 1 (Document IDC#231153). *IDC.*	December 2011
MADDEN, B., KNUTH, G. and MADDEN, J. 2012. The VDI Delusion.	2012
MEHRA, ROHIT, Competitive Analysis, IDC Marketscape: Worldwide Enterprise WLAN 2011- 2012 Vendor Analysis, Volume 1 (Document # 231686). IDC.	December 2011
MICHAEL J. KING, TIM ZIMMERMAN. 2011. Magic Quadrant For Wireless LAN infrastructure, March 2011 (Document # G00210047). *Gartner*.	March 11
NETWORKWORLD. 2010. VMware disses bare-metal desktop hypervisors. Available at: http://www.networkworld.com/news/2010/083110-vmware-desktop-hypervisors.html	Accessed: 21st June 2012

OMA. 2012. Mobile Location Protocol V3.1. Available at: http://www.openmobilealliance.org/technical/release_program/mlp_v31.aspx	Accessed: 13th June 2012
OPSI. 2012. Opsi Client Management System. Available at: http://www.opsi.org/en	Accessed 22nd June 2012
SONG, I. 2011. IDC MarketScape: Worldwide Desktop Virtualization 2011 Vendor Analysis (Document # 228619). *IDC.*	June 11
SPRUIJT, R. 2012 b. User Environment Management Smackdown – Version 1.2. *PQR*.	January 2012
SPRUIJT, R., 2012 a. VDI Smackdown! – Version 1.3. *PQR*.	February 2012
TRONI, F. and MARGEVICIUS, M. 2010. Total Cost of Ownership Comparison of PCs With Server-Based Computing, 2011 Update (Document # G00209456). *Gartner*.	December 2010
TRONI, F., MARGEVICIUS, M. and SILVER, M. A. 2010. Total Cost Of ownership comparison of PC's with Server-Based computing (Document # G00159622). *Gartner*.	August 2010
TRONI, F.2011. Notebook Total Cost of Ownership updated: 2011 (Document # G00208793). *Gartner*.	November 2010
VLACIL, P. and BESTAK, R. 2009. Implementing Mobile Location Protocol. Available at: http://www.rdc.cz/download/publications/vlacil_petr_tsp_2009.pdf	Accessed: 13th June 2012
W3. 1999. Web Content Accessibility Guidelines 1.0. Available at: http://www.w3.org/TR/WCAG10/	Accessed: 31st May 2012
W3. 2010. What is HTML. Available at: http://www.w3.org/TR/WCAG10/	Accessed: 13th June 2012
W3.2012. Mobile Web Application Best Practices. Available at: http://www.w3.org/TR/mwabp/	Accessed: 1st June 2012
WEBCREDIBLE. 2012. Improving usability for screen reader users. Available at: http://www.webcredible.co.uk/user-friendly-resources/web-accessibility/screen-readers.shtml	Accessed: 31st May 2012

4 GLOSSARY

Reference	Meaning
AP	Access Point
AV	Anti-Virus
BIL	Business Impact Levels
BYOD	Bring Your Own Device
CI	Configuration Item
CMDB	Configuration Management Database
COTS	Commercial off the Shelf
CSS	Cascaded Style Sheets
DOM	Document Object Model
DPL	Data Loss Prevention
HTML	Hyper Text Markup Language
HVD	Hosted Virtual Desktop
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IL	Impact Level, a.k.a. Business Impact Level is a standardised means of assessing the business impact of loss of confidentiality, integrity or availability of business assets owned, ranging from 0 (lowest) to 6 (highest).
IPC	Information and Protection Control
JVM	Java Virtual Machine
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LoB	Line of Business
Local Computing	When the application is installed and run locally and all the computing is done on the client side. For example, running a Microsoft Office application on a laptop.

MAM	Mobile Asset Management
MDM	Mobile Device Management
MDP	Mobile Data Protection
OS	Operating System
RDP	Remote Display Protocol
Remote Computing	When the application is run remotely and all the computing is done on the server side. For example, accessing an HR or timesheet applications that is run remotely on the server.
RF	Radio Frequency
RIA	Rich Internet Applications
SaaS	Software-as-a-Service
SBC	Server-Based Computing
SCEP	Simple Certificate Enrolment Protocol
SDK	Software Development Kit
SOAP	Simple Object Access Protocol
TCO	Total Cost of Ownership
THICK OS	Operating System than runs on a Thick-Client Device (e.g. a laptop or a desktop). Examples of thick OS include Microsoft Windows, Unix, Linux, and OSX.
THIN OS	Operating System that runs on a Thin Client Device, or an operating system that is installed on a thick-client device in order to re-purpose it as a thin client, for example Windows Thin PC.
TLS	Transport Layer Security
TS	Terminal Service
UDDI	Universal Description, Discovery and Integration
UEM	User Environment Management
USV	User State Virtualisation
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network

W3C	World Wide Web Consortium
WAM	Web Availability Management
WCAG	Web Content Accessibility Guidelines
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WLAN IPS	WLAN Intrusion Prevention System
WPA	Wi-Fi Protected Access
WSDL	Web Services Description Language
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language