# *Government ICT Strategy*

# *End User Device Programme*

# *EUD Technical Framework Document – Phase 3*

## *Protective Marking: Unclassified*

***(v1.1) – Part 2***

**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 the document as per review feedback by CESG |
| 0.5 | September 2012 | Revised the structure and document as per feedback from Nigel |
| 0.6 | September 2012 | Revised the draft as per feedback from Peer Review meeting |
| 0.7 | September 2012 | Removed vendor product details 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 2 of the 3 part 'EUD Technical Framework Document Release 3'. It continues directly from part 1 of the document and contains the first section of the appendix (section 6) which is referenced in Parts 1 and 3.**

# 6 APPENDIX

## 6.1 SOLUTION GUIDELINES

The EUD Framework Level 3 analyses each Level 2 component and 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 lightboard below shows the components of the framework.

The Level 3 Framework provides Solution Guidelines for government organisations and suppliers to use during all phases of an IT transformation programme.

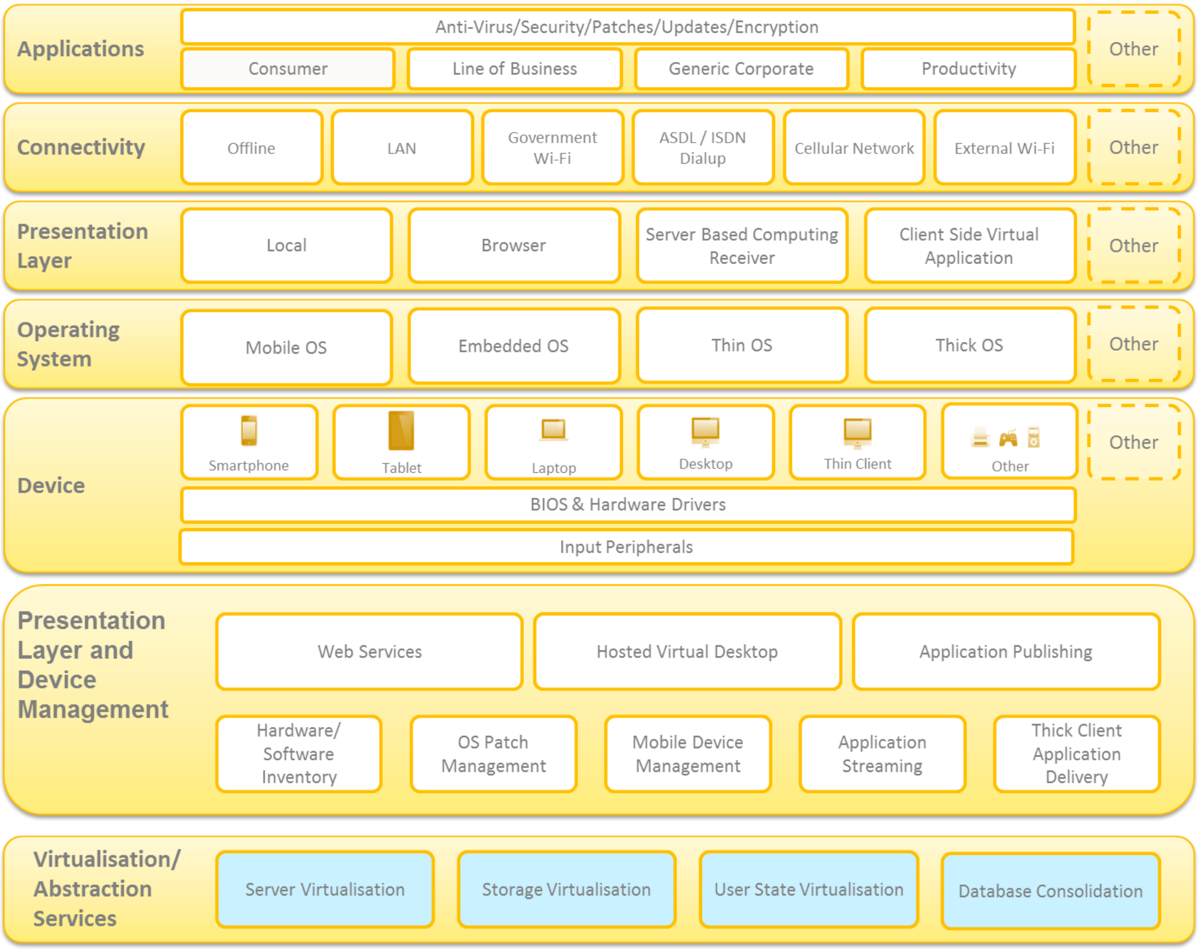


**FIGURE 1 – FRAMEWORK LIGHTBOARD SHOWING ALL COMPONENTS**

This section will:

- Introduce the Application, Connectivity and Operating System layers.
- Provide in-depth analysis on the various technologies present under Presentation Layer such as Server Based Computing, Client Side Virtual Application and Browser / Webs Services Based Model.

- Provide details around Device Management and the available End User Devices. This includes:
  - Desktops and Hybrid Desktops;
  - Thin Clients (including Repurposed PCs)
  - Laptops
  - Tablets
  - Smartphones

### 6.1.1 Applications Layer

The End User Device Framework Conceptual Framework (Level 1 and 2) introduced the components of the Application Layer. The introduction is repeated below for ease of reference but can be found in its original context at:

http://www.cabinetoffice.gov.uk/sites/default/files/resources/End-User-Device-Programme-Conceptual-Framework-Release-1-4_0.pdf

The Framework groups most applications into 4 distinct categories. These are detailed below with the appropriate definition.

- **Consumer**- Consumer Applications are available on Applications Markets that are intended for individuals as opposed to organisations or institutions. These may help with the user's work-related activities e.g. file sharing or part of their home life e.g. music or social networking applications.
- **Line of Business**- A set of critical computer applications vital to running a given business area.
- **Generic Corporate Systems** refers to those services which all employees need to access at some point, such as HR systems for booking leave, claiming travel expenses etc.
- **Productivity**- An application that is common to most computers in an organisation and used primarily by knowledge workers, such as word processing or internet browsing.

### 6.1.2 Connectivity Layer

The End User Device Framework Conceptual Framework (Level 1 and 2) introduced the components of the Connectivity Layer. The introduction is repeated below for ease of reference but can be found in its original context at:

http://www.cabinetoffice.gov.uk/sites/default/files/resources/End-User-Device-Programme-Conceptual-Framework-Release-1-4_0.pdf

The Frameworks details potential connectivity routes for each device and user. These are defined as follows.

- **Offline**- The device operating without any form of connection to the internet, intranet or other devices.
- **LAN**- Wired LAN Wired Ethernet connectivity to PSN on Government premises.
- **Government WiFi**- Internal wireless ethernet connectivity on Government premises.
- **ADSL/ ISDN/ Dialup**- Connectivity to the internet or the company network over the public telephone network.

- **Cellular Network**- Connection to the internet via non-Government, publicly available mobile phone networks.
- **External WiFi**- Access through wi-fi hotspot networks, normally in a public location such as a café.

### 6.1.3 Presentation Layer

The End User Device Framework Conceptual Framework (Level 1 and 2) introduced the various components of the Presentation Layer - Local, Browser, Server Based Computing and Client Side Application Virtualisation. This can be found here:

http://www.cabinetoffice.gov.uk/sites/default/files/resources/End-User-Device-Programme-Conceptual-Framework-Release-1-4_0.pdf

This section will discuss in detail the benefits, limitations and key considerations for the following technological components:

- Server Based Computing
- Client Side Virtual Application
- Browser / Web Services Based Model

#### 6.1.3.1 Server Based Computing

Application virtualisation using Server Based Computing has the potential to reduce the total cost of ownership when implemented in the right environment and with the right group of users. The typical benefits of virtualisation are security, flexibility and ease of supportability. According to analysis done by Gartner (TRONI & MARGEVICIUS, 2010) the greatest benefit will arise when the virtualisation of an application is applied to an unmanaged desktop environment. Any cost savings will be much less clear cut if the existing environment is well managed.

In Server Based Computing (a type of desktop virtualisation), end-user applications are hosted on servers, executed remotely and presented to thin client devices via a remote display protocol, such as Linux/Unix X11R6 or XDMCP (open source options), Microsoft RDP, Citrix ICA/HDX or VMware 'PC-over-IP'). Users working on thin clients connect to the server via a display protocol which then starts a remote desktop on the server and presents it to the thin client. The following diagram shows the options available under Server Based Computing:

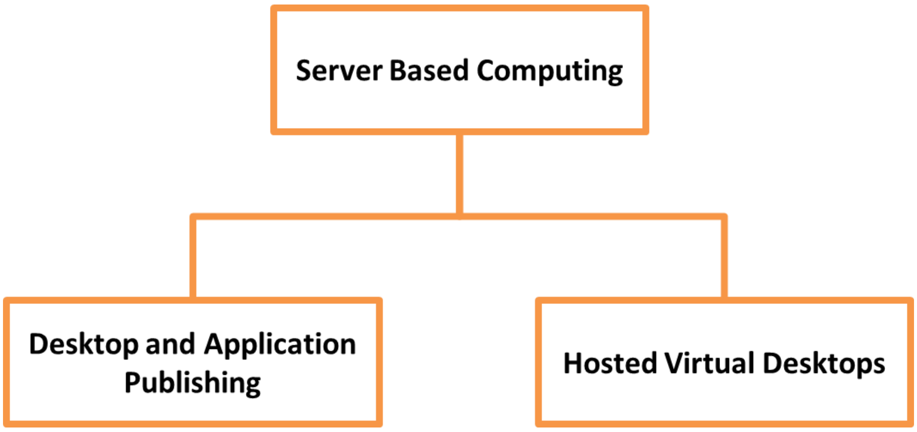


FIGURE 2 – OPTIONS FOR SERVER BASED COMPUTING

## Desktop and Application Publishing

Desktop and Application Publishing (also known as Shared Remote Desktop) is a solution for gaining remote access to desktops and applications that are executed on a server in the data centre. The execution of the applications takes place centrally and the information is displayed on the client's screen via remote display. A Server Based Computing Receiver (the client side component of Server Based Computing delivery method which can run on both thin and traditional thick clients) is installed on the device to receive a data stream from the server. On the server, every user can have their own desktop session and can share the computer platform with other users. The following diagram describes the Desktop and Application Publishing solution.

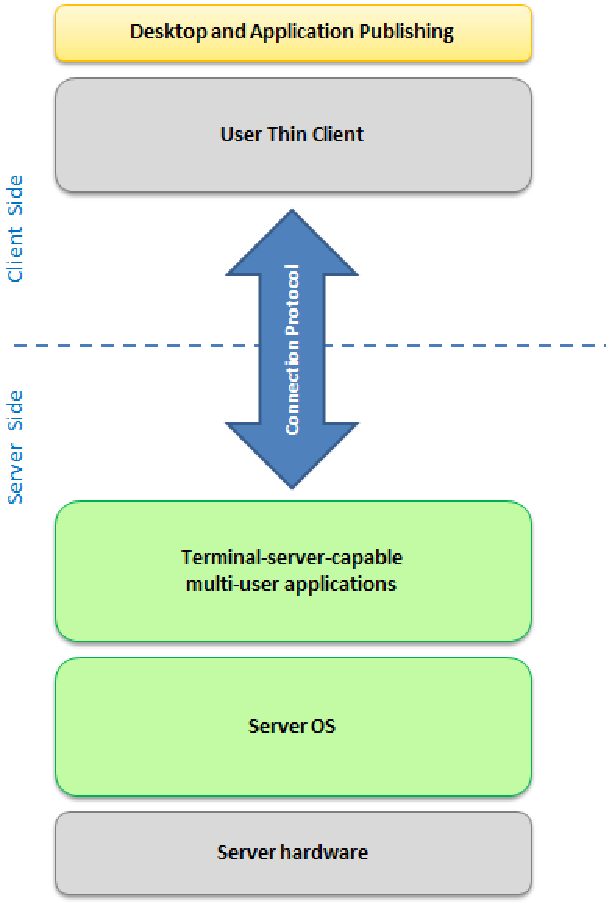

Desktop and Application Publishing
User Thin Client
Client Side
Connection Protocol
Server Side
Terminal-server-capable multi-user applications
Server OS
Server hardware

FIGURE 3 – DESKTOP AND APPLICATION PUBLISHING

The table below details the typical advantages of a Desktop and Application Publishing solution:

| Area | Key Benefits |
|---|---|
| **Cost** | • Provides a cheaper implementation in comparison to Hosted Virtual Desktop solutions as less datacentre hardware is required. |
| **Deployment** | • Enables the easy roll-out of applications to users, who use the same stack of applications. |
| **Support and Management** | • Delivers efficient management of branch office infrastructure. |

| | |
|---|---|
| **Hardware Requirements** | - Using shared resources can result in more users working on the same physical hardware. |

TABLE 1 – BENEFITS OF DESKTOP AND APPLICATION PUBLISHING SOLUTION

The following are the typical limitations of a Desktop and Application Publishing solution:

| **Area** | **Key Limitations** |
|---|---|
| **Cost** | - New deployments can be expensive due to the costs associated with infrastructure hosting space, servers, software and networking. |
| **Performance** | - Performance can degrade as the number of user per server increases. Performance can also degrade as a result of a high number of applications being used. A careful focus on capacity management and scaling out the solution to maintain service quality is needed. |
| **Network Bandwidth** | - This model requires excellent network connection and server performance and capacity to produce a good user experience. |
| **Business Continuity** | - Requires redundant servers in the data centre to provide failover. The complete loss of network connectivity or failure of the data centre will render the clients inoperable. |

TABLE 2 – LIMITATIONS OF DESKTOP AND APPLICATION PUBLISHING SOLUTION

### Key Considerations for Desktop and Application Publishing

The table below sets out the features that organisations should consider when choosing a Desktop and Application Publishing solution.

| **Attributes** | **Key Considerations** |
|---|---|
| **Accessibility** | - A user should be able to log on at any workstation in the organisation. |
| **User Experience** | - Overall user experience must be broadly equal to that on a thick client device.<br>- The solution should be capable of delivering a rich multimedia experience at the endpoint i.e. not preclude content that would facilitate new ways of working. |
| **Availability** | - The solution should meet user's expectation for availability, i.e. no limitations caused by poor or unreliable networks or failures in the data centre. |
| **Support and** | - Ability to support open standard protocols. |

| | |
|---|---|
| **Management** | • Ease of installation, use and management.<br>• Availability of centralised management features likes application / user profile management, policy based management etc. |
| **Security** | • Availability of key security features like secure application access, encrypted delivery, multi-factor authentication etc.<br>• Options to centrally manage security configurations and an ability to manage the location of data. |
| **Remote App and Desktop Connections** | • Options to have both a full screen remote desktop and access to stand-alone remote published applications. |
| **Scalability** | • Ability to scale-up with increased load as a result of organic growth, mergers or actuations.<br>• Ability to cope with daily peaks e.g. everyone logging in between 0900 and 0930. |
| **Remote access** | • Availability of online and offline application access. |

TABLE 3 – KEY CONSIDERATIONS FOR DESKTOP AND APPLICATION PUBLISHING

## Hosted Virtual Desktops

Hosted Virtual Desktops also known as Virtual Desktop Infrastructure (VDI) is a solution for remotely accessing desktops that are executed on a virtual server in a data centre. The servers are loaded with a Hypervisor, which allows multiple Operating Systems to run concurrently on the host server. The Hypervisor completely separates the virtual desktops from the underlying and similar virtual Operating Systems. The virtual infrastructure ensures availability and manageability. This type of virtualisation relies on hosting full client operating system in the data centre which can provide a full desktop OS experience with all features a user may require. Programme execution, data processing and data storage take place centrally on this desktop. The information is displayed on the client's thin client device via a remote display protocol such as Linux/Unix X11R6 or XDMCP (open source options), Microsoft RDP, Citrix ICA/HDX or VMware 'PC-over-IP'. The following diagram illustrates the Virtual Desktop Infrastructure:

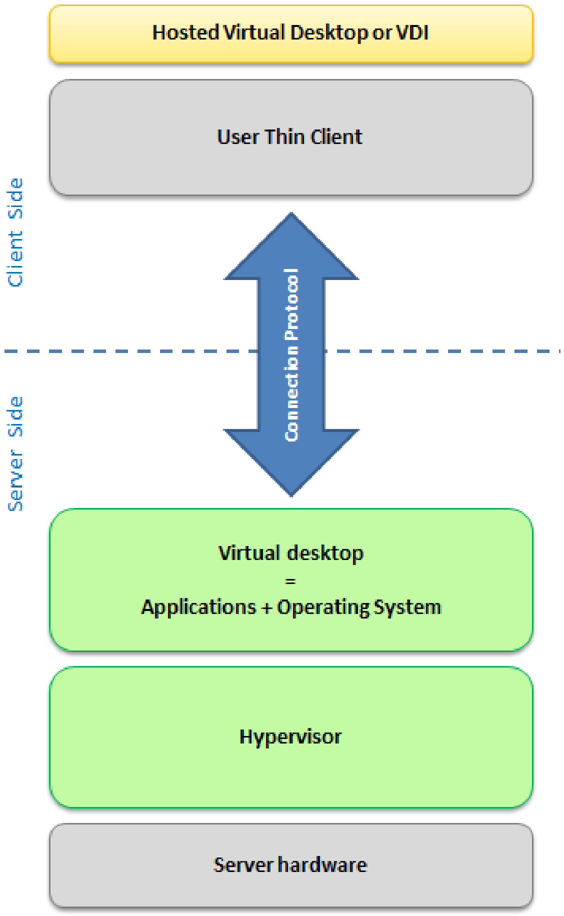


FIGURE 4 – HOSTED VIRTUAL DESKTOP

A hosted Virtual Desktop typically falls into one of the following 3 categories:

1. Persistent Desktops
2. Non-persistent Desktops
3. Layered Desktops

**Persistent Desktops** – Also known as 'stateful' desktops. Here, the users are assigned to dedicated virtual machines, where they will have the ability to install the software, make any workspace related changes and save them in between sessions. These changes will then be retained when the user logs in the next time.

| Pros | Cons |
|---|---|
| • The user can install software on the virtual machine and it will be retained when they log back in again.<br>• Any changes to the OS will be maintained between system reboots. | • High cost of storage maintenance required to implement thick virtual machines for every user.<br>• Little opportunity for operational cost savings, as the virtual machines are managed similar to physical PCs. |

TABLE 4 – PROS AND CONS OF PERSISTENT DESKTOPS

**Non-Persistent Desktops –** Also known as 'stateless' desktops. Here, users are assigned to a virtual machine that is same every time they login. It means that the desktops will always revert back to their original state after users have logged-off, meaning changes made by users on the desktop between different sessions are not retained.

| Pros | Cons |
|---|---|
| • Simple roll-out and ease of update of basic images.<br>• All virtual desktops are 100% identical.<br>• The user always has a clean desktop.<br>• Less management effort in supporting non-persistent desktops as all the images are standardised.<br>• Less storage space is required as a single base OS image can be shared across many desktops. | • Any customisations made by the users are lost after each user session.<br>• Applications that are delivered outside of the base image by IT are lost after each desktop reboot. |

TABLE 5 – PROS AND CONS OF NON-PERSISTENT DESKTOPS

**Layered Desktops -** This combines the benefit of both persistent and non-persistent desktops. Here, persistent virtual machines are assigned to every user, which ensures that all changes made by the users will be retained through reboots. However, the persistent virtual machines are dynamically constructed from a shared, reusable set of stateless OS and Application layers that can only be created and assigned by IT.

| Pros | Cons |
|---|---|
| • The user can install software on the virtual machine and it will be retained when they log back in again.<br>• Simple roll-out and ease of update of basic images.<br>• All virtual desktops are 100% identical.<br>• The user can be reverted back to a clean desktop.<br>• Less management effort in supporting this due to standardisation of images, simpler application packaging and ability to rollback OS and application packages.<br>• Less storage space is required as a single base OS image and single image of common applications can be shared across many desktops. | • A relatively new technology and so has not been implemented on a wider scale to many real world customers. |

TABLE 6– PROS AND CONS OF LAYERED DESKTOPS

The table below details the typical advantages of Hosted Virtual Desktops:

| Area | Key Benefits |
|---|---|
| **Security** | • Provides increased security as the Operating System, applications and data are stored in the data centre. |
| **Support and Management** | • Centralised management and administration for desktop images and applications. |
| **Performance** | • Can provide a consistent performance when accessed from different locations (provided network connectivity is good). |

TABLE 7 – BENEFITS OF HOSTED VIRTUAL DESKTOPS

The following are the typical limitations of Hosted Virtual Desktops:

| Area | Key Limitations |
|---|---|
| **Cost** | • New deployments are expensive due to the costs involving space, servers, software and networking. This is the most server-intensive delivery method. |
| **Performance** | • Performance degrades as the number of user per server increases. |
| **Bandwidth** | • Good bandwidth required to maintain display, keyboard and mouse responsiveness. A careful focus on capacity management to maintain service quality is needed. |
| **Software Compatibility** | • Not all software or specialised peripherals are compatible with this approach. |
| **Business Continuity** | • Requires redundant servers in the data centre to provide failover. The complete loss of network connectivity or failure of the data centre will render the clients inoperable. |
| **Capacity** | • This approach requires more capacity per user than the shared server-based computing approach outlined above. |

TABLE 8 – LIMITATIONS OF HOSTED VIRTUAL DESKTOPS

Hosted Virtual Desktop environment is an exception and often an expensive option. Organisations usually choose to go for this option for the following reasons:

- To enable users to work from anywhere.
- To allow users to choose any devices.
- To allow users to install software.
- To deliver existing applications to new devices.
- To facilitate a change of operating system by allowing old applications to run on a different OS.

### Key Considerations for Hosted Virtual Desktops

The table below sets out the features that organisations should consider when choosing a Hosted Virtual Desktop solution.

| Attributes | Key Considerations |
|---|---|
| **Local Dependent Connectivity** | • The solution should be easily accessible irrespective of user's location. |
| **User Experience** | • Overall user experience must be broadly equal to that on a thick client device.<br>• The solution should be capable of delivering a rich multimedia experience at the endpoint. |
| **Support and Management** | • Ease of installation, use and management.<br>• Availability of wizard based management.<br>• Ability to support open standard protocols.<br>• Availability of key features likes application publishing, monitoring, reporting, user profile management, bandwidth management and resource management.<br>• Support for Guest (VM) OS support and Client (endpoint) OS support.<br>• Support for hypervisors.<br>• Ability to support various browsers.<br>• Availability of the skilled resources in the market place to implement and support the product. |
| **Security** | • Availability of key security features like secure application access, encrypted delivery, multi-factor authentication etc.<br>• Options to centrally manage security configurations and an ability to manage the location of data. |
| **Scalability** | • Ability to scale-up with increased load as a result of organic growth, mergers or actuations. |
| **Software Compatibility** | • Ensure the software is compatible with the solution. |

TABLE 9 – KEY CONSIDERATIONS FOR HOSTED VIRTUAL DESKTOPS

#### 6.1.3.2 Client Side Virtual Application

Client Side Virtual Application is a process by which applications are streamed to the client device from a central location and executed locally. The streamed application does not make any change to the underlying operating system registry and typically only interacts with a receiver to provide user interface.

This is best suited for environments where application deployment and license management are critical. The IT administrator can use policies to control when licenses expire and whether a PC is connected to the network or not. For example, licenses can be set to expire for temporary or contract employees when their contracts end. IT can then repurpose the license. Applications can be streamed to a compatible operating system hosted on any delivery platform, whether it is virtualised in the data centre, locally on a physical PC or a terminal server.

Client Side Virtual Application reduces application conflicts for local as well as streamed applications, as virtualised applications run within an isolated container and do not make any changes to the underlying OS. The streamed application can be cached locally and the user can work offline and then synchronise later when online.

The table below details the typical advantages of a Client Side Virtual Application solution:

| Area | Key Benefits |
|---|---|
| **Support and Management** | • Streamed applications can be managed centrally and used to resolve situations where legacy or bespoke applications cause conflicts.<br>• The applications can be streamed to a thin or thick client. If the application is to be used offline an intelligent OS is required for caching the streamed application. |
| **Business Continuity** | • Disaster recovery and business continuity processes can be simplified as users can readily access applications from a different location, if a primary site is unavailable. |
| **Security** | • Applications are normally stored in the datacentre and therefore secured by higher level security protocols. |
| **Performance** | • The general performance of application after launch is as good as locally installed application. (Streamed / virtualised applications place added demand on network bandwidth). |

TABLE 10 – BENEFITS OF CLIENT SIDE VIRTUAL APPLICATION

## Key Considerations for Client Side Virtual Application

The table below sets out the features that organisations should consider when choosing a client side virtual application solution.

| Attributes | Key Considerations |
|---|---|

| | |
|---|---|
| **Security** | • Ensure that at runtime data and application are not vulnerable to client side attack or theft.<br>• Local corruption is minimised and patches are updated at each initiation from the streaming server.<br>• Inherently isolating application minimises data corruption. |
| **Manageability** | • Central management of application licencing and provisioning<br>• Where compatible, virtualisation will allow legacy applications to run on a newer operating system<br>• When implemented correctly application streaming / virtualisation reduced conflicts, corruption, and randomness in the operating system registry. |
| **Performance** | • Streaming download speeds can be affected by distance from server, network load, and number of users interacting.<br>• Can suffer from "storms of activity" when many users log in at the same time, however after launch network demand typically drops to a very low level.<br>• The general performance of application after launch is as good as locally installed application. |
| **Infrastructure Cost** | • Not all software is suitable for application streaming / virtualisation. Initial sequencing setup/debugging can be time and labour intensive.<br>• At times streamed and virtualised application interactions can be challenging.<br>• Generally lower cost of deployment as compared to centralised computing models.<br>• Fewer less costly servers needed for base infrastructure. |
| **Disaster Recovery** | • Streamed applications can be used in cached mode for offline use and increased mobility<br>• Virtual or streamed application servers can be accessed through different location if the primary location is unavailable.<br>• High demand on bandwidth for initial launch of applications in a disaster scenario as all users will try to access application at same time. |
| **Offline Availability** | • Streamed application can be cached locally and the user should be able to work offline and then synchronise later when online. |

TABLE 11: KEY CONSIDERATIONS FOR CLIENT SIDE VIRTUAL APPLICATION SOLUTION

### 6.1.3.3 Browser / Web Services Based Model

Web browsers are software applications that locate, retrieve and display the content present on either the World Wide Web or on the organisations internal network. As in a client / server model, the browser is a client that resides on the end user's device and contacts the web server for the required information. The web server sends information back to the web browser which displays the results on the device. A web browser can be used to access web applications from any end user device including desktops, laptops, thin clients, tablets and smartphones.

!

**Important Note**

A Web application is an application that can be accessed over the internet or intranet using only a web browser. From organisational perspective, it can also mean a software application that is coded in a browser-supported language and that is reliant on a web browser to render the application interface.

Web applications are popular because users can conveniently access them through web browsers on most devices. However, organisations need to be wary of the differing levels of standards compliance within the various browsers and avoid lock in to proprietary browser plug-in architectures. Web applications should be designed to be W3C standard compliant and browser vendor agnostic. Web applications are easier to update and maintain in comparison to the traditional method of installing the applications on individual user's device and updating them on regular basis. The following list details the typical benefits of using web applications through browsers:

- It is easy to roll-out web applications in a large organisation as a modern standards compliant web browser is all that is required.
- Browser based applications typically require little or no disk space on the end user device.
- Web applications do not require any upgrade at the client end as all the features are implemented on the server and delivered automatically to the users.
- Web applications provide cross-platform compatibility (i.e. compatible with Windows, Mac, Linux, etc.) as they operate within a web browser environment.

The following are the typical drawbacks of using web applications through browsers:

- Web interfaces may not be as sophisticated by comparison with a thick client interface and can deliver a limited user experience. This is a rapidly diminishing problem as modern web standards and technologies enable very rich interfaces and a fluid user experience.
- Web applications require persistent network connectivity to run effectively. If the connectivity is interrupted, then the application will no longer be usable.

There are certain web development standards and considerations that need to be taken into account for writing web applications. More details around web development standards, legacy web application compatibility, and performance can be found in section 6.6. It is important to note that browsers do not conform to all specifications provided by standards. Some browsers introduce their own HTML tags, for example, in order to achieve extra functionality and not all web applications work in the same way in every browser. Furthermore, certain applications may require specific browsers or require a minimum version level for them.

Both cloud and mobile technology trends are enabled by web based service provision, and this should be reflected in the design of IT solutions. Similarly, decoupling applications from specific end user devices or operating systems is a key goal for the government ICT strategy.

## Browser / Web Services Considerations

The table below highlights the desirable attributes for browsers / web services.

| Attributes | Key Considerations |
|---|---|
| **Supported Platforms** | • Ability to work on different operating systems like Windows, Mac OS, Linux etc. |
| **Form Factors** | • Ability to work on different devices like desktops, laptops, tablets, smartphones etc. |
| **Functional Efficiency** | • Ability to open websites on different tabs.<br>• Availability of an integrated search engine. |
| **Customization** | • Ability to change the look and feel of the browser.<br>• Ability to install any add-ons or plug-inn software to customize the browser (subject to local policy and the baseline security build for applications). |
| **Performance** | • Responsiveness and speed of the delivery of web services. |
| **Admin Efficiency** | • Ability of the browser to update itself automatically on a regular basis.<br>• Release of the security patches and fixes to be rolled out centrally and on a frequent basis. |
| **Security** | • Availability of key security features like anti-spyware, anti-virus, anti-phishing, pop-up blocking and privacy mode. |
| **Support** | • Support for most of the recent web standards.<br>• Support for different devices like desktops, laptops, smart phones & tablets.<br>• Availability of a built in support community to provide support for and resolve any technical issues. |

TABLE 12 – KEY BROWSER / WEB SERVICES CONSIDERATIONS

W3schools maintains current statistical information about web browsers which can be found at this link: http://www.w3schools.com/browsers/browsers_stats.asp.

### 6.1.4 Operating System Layer

The End User Device Framework Conceptual Framework (Level 1 and 2) introduced the components of the Operating System Layer. The introduction is repeated below for ease of reference but can be found in its original context at:

http://www.cabinetoffice.gov.uk/sites/default/files/resources/End-User-Device-Programme-Conceptual-Framework-Release-1-4_0.pdf

The conceptual framework identifies the type of Operating System for each device. The Operating Systems relevant for current scope are Mobile OS, Thin OS and Thick OS, however all the different categories are described below:

- **Mobile OS-** A mobile operating system (Mobile OS) is the operating system that controls a smartphone, tablet, PDA, or other mobile device. Modern mobile operating systems combine the features of a personal computer operating system with touchscreen, cellular, Bluetooth, WiFi, GPS (Global Positioning System) mobile navigation, camera, video camera, speech recognition, voice recorder, music player, near field communication, personal digital assistant (PDA), and other features. Examples of Mobile OS include Apple iOS, Android, Blackberry, Windows 7 and Symbian.
- **Embedded OS**- An embedded operating system performs a very specific purpose to the exclusion of all other functions. These systems are narrow purpose, fixed-function computer systems. An important difference between most embedded operating systems and desktop operating systems is that a standard desktop operating system creates an environment where a user and the computer may interact with one another to perform a huge variety of tasks, whereas an embedded operating system will only perform one type of task and it will often do it without any user intervention. An embedded operating system is also known as real-time operating systems (RTOS) and is typically a part of embedded computer systems.
- **Thin OS**- A Thin OS is an stripped down Operating System that runs on a Thin Client Device and helps to boot up the system and connect to a server that will project VDI or RHS. 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.
- **Thick OS**- A Thick OS is an 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.

### 6.1.5 Device Management and Device Introduction

This section introduces the concepts behind device management. Central device management has typically been a key element with enterprise IT solutions. Adopting the user centric approach outlined in the EUD Framework creates the opportunity for certain groups or users to “self-serve” and manage the device themselves. An organisation however will need to carefully assess the risks and determine which elements of central device management must remain in place (for example remote wipe for a lost device).

!

**Important Note**

ITIL is an industry standard approach for IT Service Management. When considering device support ITIL should be used to inform your chosen solution. For more information about ITIL, visit the official website here: http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

#### 6.1.5.1 Device Management Considerations

Managing devices is a fundamental part of ICT administration but with an increasing mix of available devices, it can be challenging task. The management processes and tools control how secure an organisations devices are, how often they are patched, how hardware and software inventories are managed, how agile and responsive an organisation is to any potential cyber threats and how effectively the device lifecycle is managed.

Device management applies to laptops and desktops and is increasingly extended to smartphones, tablets and other mobile devices. Good device management involves installing and maintaining hardware and software, ensuring the security and connectivity, and knowing the state of a device.

Gartner describes flavours of device management that vary from being “lightly managed and wide open” to “well-managed and locked down”. The table below highlights the fundamental differences between these environments and can be used as a checklist to establish how well-managed an organisation’s EUD environment is and where it might be improved.

| **Device Management** | | | |
|---|---|---|---|
| **Activities** | **Lightly Managed** | **Moderately Managed** | **Well-Managed** |
| **OS Deployment** | Local | Centralised | Centralised |
| **Application Deployment** | Local | Centralised /Local | Centralised |
| **Patch Management** | Local | Centralised | Centralised |
| **AV Management** | Local | Centralised | Centralised |
| **Hardware and Software Inventory** | Manual | Automatic | Automatic |
| **Monitoring** | Reactive | Pro-Active | Pro-Active |
| **User Rights on local Machine** | Admin | Power User | Basic User |

| | | | |
|---|---|---|---|
| **Processes and Policies** | Not Defined | Loosely Defined | Very well Defined |
| **Integration with CMDB** | No Integration | Some Integration | Some Integration |
| **OS Lockdown** | User can change settings | User can change some settings | Complete lockdown |
| **USV (User State Virtualisation)** | Local user state | No USV | Desirable |
| **Application Virtualisation** | No Application Virtualisation | Desirable | Desirable |

TABLE 13 – EUD MANAGEMENT ENVIRONMENTS

Mature products exist for managing desktops, laptops and server environments but the technology for managing mobile devices, such as smartphones and tablets, is still developing. While the leading products in the device management market are now being extended to support mobile devices, many organisations have opted for specialist products to manage their mobile devices and separate products to manage rest of the environment. A further discussion of mobile device management is detailed in the “Additional Support and Management considerations for Smartphones and Tablets” section below.

This document examines well-managed devices focusing on desktops and laptops, although many of the principles can also be extended to other devices. Section 7 (part 3 of this document) covers the components for each of six End User Device User Profiles.

Gartner provide an analytical view on savings gained from well-managed desktop environments and report on the Total Cost of Ownership (TCO) of desktops and laptops compared to Server-Based computing (TRONI, 2011., TRONI, MARGEVICIUS and SILVER, 2010., TRONI and MARGEVICIUS, 2010) The reports show that comprehensive TCO savings and direct cost savings can be achieved when organisations adopt a well-managed desktop environment.

This finding is supported by Brian Madden in ‘The VDI Delusion’ (MADDEN, KNUTH, & MADDEN, 2012) who argues that potential cost savings attributed to Virtual Desktop Infrastructure (VDI) can also be realised by locked down and well managed desktops.

In short, a well-managed desktop environment reduces risks, improves productivity, reduces accidental loss of intellectual property, improves accountability, reduces IT support activities and reduces business impact during end user device failure. The implementation of well managed desktop will be covered in the specific Solution Implementation Guidelines in section 6.2 of this document.

## Centralised Device Management

Centralised desktop management or centralised client management is a function that allows organisations to manage their computer infrastructure centrally. This is achieved by a set of software tools, commonly known as client management tools, which enable organisations to deploy, stream, manage, support, track and automate repetitive tasks.

### Key Consideration for Client Management Tools

Below are the features that organisations should consider when choosing a client management tool for managing end user devices.

| Attributes | Key Considerations |
|---|---|
| **Platform Support** | • Functionality to automatically deploy an Operating System to remote clients across different networks, particularly security related patches and anti-virus definitions.<br>• Ability to distribute software to clients from a central location with minimum administrative effort and limited user involvement.<br>• Support for deploying different vendor and open source operating systems to devices (laptops, desktops and servers).<br>• Ability to manage and support varied devices (laptops, desktops, servers, tablets and smart phones). |
| **Infrastructure Management Support** | • Ability to keep centralised up-to-date inventory of client devices and support for asset discovery.<br>• Ability to maintain up-to-date software on client devices by providing centralised patch management functionality.<br>• Interoperability and integration with other systems such as third party application virtualisation or security configuration systems.<br>• Scripting, software packaging, power management, software usage monitoring and remote control support.<br>• Software usage monitoring and license management.<br>• Easy to use centralised management console.<br>• Ability to manage device configuration and policy. |
| **Scalability** | • Ability to scale-up with increased load as a result of organic growth, mergers or actuations.<br>• Ability to operate agentless.<br>• Support for multiple configuration and management consoles. |

| | |
|---|---|
| **Training and Skillset** | • Readily available product training from vendors.<br>• Readily available expertise in the market place to implement and support the product.<br>• Structured documentation available for the product implementation, support and maintenance. |
| **Security** | • Granular security options available to provide different levels of access to groups and individuals.<br>• Safeguard from accidental configuration changes or deletion or push of policies across infrastructure platform. |

TABLE 14: KEY CONSIDERATIONS FOR CLIENT MANAGEMENT TOOLS

### Additional Key Considerations for Thin Client Support and Management

The table below highlights the desirable attributes and key considerations for client management tools.

| Attributes | Key Considerations |
|---|---|
| **Configuration and Management of devices** | • Easy and simple processes for real time asset management.<br>• Centralised configuration, upgrade and trouble-shooting facility.<br>• Availability of wizard based console to carry out the above tasks. |
| **Security** | • Availability of secure HTTPS-based communication.<br>• Availability of compliance and policy based security management. |
| **Scalability** | • Scalable to support many clients. This number should be in the thousands and an organisation should assess its requirements when deciding the threshold. |
| **Deployment and Training** | • Simplified device deployment and task automation.<br>• Availability of quick reference guides to help through the various processes. |

TABLE 15 – KEY SUPPORT AND MANAGEMENT CONSIDERATIONS FOR THIN CLIENT

### Additional Support and Management considerations for Smartphones and Tablets

Providing secure, stable and accessible smartphones and tablets requires well-planned support and management. Many enterprises are embracing mobile devices as critical to business success. However, in a rapidly-changing landscape, these devices pose unique challenges. This section of the

Framework outlines the key points that organisations should consider to support and manage smartphones and tablet devices.

! **Important Note**

Organisations should also ensure that they comply with the relevant CESG Good Practice Guides and Policies and Standards relating to EUD (CESG, 2012).

Available at: http://www.cesg.gov.uk/PolicyGuidance/Pages/index.aspx.

### 1. Configuration Management / Asset Inventory Management

Mobile device management is a complex task that needs to be carefully controlled. As mobile devices are cheap and easily accessible, the number of such devices tends to increase rapidly. To cope with this increasing demand it is important that a management application can perform all its required activities from a central location. A concise view of an organisation's assets enables administrators take quick and effective decisions that reduce operating costs.

A mobile or tablet device in an enterprise goes through number of life-cycle events. Typically these are:

- **Connection**: This is the initial phase where the device is introduced into the enterprise environment. At this stage the device may not have the applications installed on it required to carry out day-to-day business activities but is identifiable on the network and not yet ready for use.

- **Configuration:** To carry out day-to-day business activities a certain set of applications and tools need to be installed on a given device. These applications can be configured and installed remotely depending upon the user's profile. Administrators need to design application profiles based on users' requirements and run the auto-deployment tools which install tools/applications on the device based on these profiles. The capability of installing applications based on pre-configured profiles remotely makes the entire process very fast. In some cases administrators may choose to impose certain restrictions on users. For example, users could be prohibited from installing applications on the device. All these elements are driven by an organisation's management policies.

  A device may require more than one cycle of configuration during its lifespan in the enterprise environment. This depends upon the user's profile, which may change in the organisation hierarchy. Again, preconfigured profiles make this process faster and more efficient.

- **Disconnection**: When employees leave an organisation the devices assigned to them need to be disconnected from the network in a seamless manner. Administrators have to remove all organisation specific data/applications from the device without interfering with user's own personal data. All licenses and subscriptions issued to the user (and therefore device) need to be revoked and the organisation's inventory needs to be updated. These aspects can be managed with minimum effort and shortest possible time using mobile device management (MDM) suites.

There is currently limited use of such technology with government and the End User Device programme will be working with CESG, the PSN programme and others to further explore the use of such technology in the future.

## 2. Key Considerations for MDM Solutions

The table below highlights the desirable attributes for an MDM solution.

| **Attributes** | **Key Considerations** |
|---|---|
| **Support and Management** | • Availability of features for centralised configuration management, inventory management, application management etc.<br>• Ability to customise processes.<br>• Software usage monitoring and license management.<br>• Easy to use centralised management console.<br>• Ability to manage device configuration and policy.<br>• Support for Bring Your Own Devices. |
| **Platforms** | • Ability to support multiple platforms like Windows, iOS & Android. |
| **Deployment and Training** | • Ability to be acquired as software-as-a-service (SaaS) or implemented as on premise product.<br>• Readily available product training from vendors.<br>• Readily available expertise in the market place to implement and support the product.<br>• Structured documentation available for the product implementation, support and maintenance. |
| **Security** | • Availability of compliance and policy based security management.<br>• Availability of device encryption and remote wipe features. |

| | |
|---|---|
| | • Granular security options available to provide different levels of access to groups and individuals.<br>• Safeguard from accidental configuration changes or deletion or push of policies across infrastructure platform. |
| **Scalability** | • Ability to scale-up with increased load as a result of organic growth, mergers or actuations.<br>• Support for multiple configuration and management consoles. |

**TABLE 16 – KEY CONSIDERATIONS FOR THIRD PARTY VENDORS FOR MDM SOLUTION**

## User State Virtualisation

The centralise management of User data provides flexibility for administrators to manage User data at central location and provides flexibility to users by removing dependency on a single end user device. User State Virtualisation (USV) also referred to as Profile Virtualisation, Profile Management, User Virtualisation or User Environment Management, is currently a topic widely discussed by vendors. Variants of USV may include more or less user attributes for virtualisation. However, the core attributes (user profile, user documents and some personalised application settings) are common in all definitions.

User State Virtualisation centralises the management of user‘s personal settings and decouples the user settings from the underlying Operating System and hardware. This allows a user’s profile and documents to be independent from the device.

The following are typical benefits of User State Virtualisation solution:

| **Area** | **Key Benefits** |
|---|---|
| **User Experience** | • Enriches the user’s experience by allowing settings to follow users across different platforms and devices. However, this is not usually possible across different operating systems or different versions of same operating system.<br>• There are vendor solutions available in the marketplace that enable cross platform and cross OS version interoperability. |
| **Mobility** | • Enables user mobility across different infrastructure solutions (the slow WAN link will affect the overall end user experience). |
| **Security** | • Application access control and user rights management.<br>• Monitoring, auditing and reporting. |

| | |
|---|---|
| **Management** | • In general simplifies user's profile administration. However, profile management will become complex with multiple platforms, multiple OS versions and multiple devices.<br>• Provides a secure and manageable environment for user profiles.<br>• Paves way for future virtualisation of other components of desktop infrastructure. |

TABLE 17 – BENEFITS OF USER STATE VIRTUALISATION

### Key considerations for User State Virtualisation

The table below sets out the features that an organisations should consider when choosing a User State Virtualisation product.

| Attributes | Key Considerations |
|---|---|
| **Management User Profile** | • Ability to virtualise user profiles so that users can save and access their customized settings (desktop, screensaver, internet favourites, and printers) on different computers within an organisation. |
| **Management User Desktop Personalisation** | • Assign drive mappings to network shares.<br>• Assign printers.<br>• Assign applications and corresponding settings.<br>• Set, change or delete registry settings.<br>• Provision specific application settings, such as Microsoft Outlook.<br>• Provision database connection settings (e.g. ODBC). |
| **Application Access Control and User Rights Management** | • Ability to enforce access to an application based on users location, time or device they are using.<br>• Ability to control which applications a user is allowed to run.<br>• This can also include blocking unknown USB devices, blacklisting websites and controlling network resources by limiting access to local drives.<br>• The ability to raise or lower admin rights on per application or task basis – based on the user. |

| | |
|---|---|
| **Resource and Application Performance Management** | • Ability to monitor and manage shared resource utilisation and take appropriate actions if threshold is breached.<br>• Ability to prevent resource draining by one user in a centralised shared environment. |
| **License Management** | • Ability to monitor the use of applications. If the application is not used the license can be revoked. |
| **Monitoring , Auditing and reporting** | • Ability to monitor, audit and report on user’s environment so that unauthorised changes are highlighted and errors and usage are reported. |

**TABLE 18: KEY CONSIDERATION FOR USER STATE VIRTUALISATION**

#### 6.1.5.2 End User Devices

This section outlines the range of devices that have been considered under the EUD Framework.

### Desktop

A Desktop PC is described as an intelligent device that is not mobile and sits on top or underneath work desk and runs full operating system. It is intended for regular use at a single trusted location. The desktop is generally connected to organisational resources via a Local Area Network and is therefore regarded as one of the safest End User Devices due to its location and trusted wired connection. A desktop is generally used as a primary tool by users who work from trusted locations using business applications to perform their day to day tasks.

### Hybrid Desktops

A Hybrid desktop is a desktop that runs a full Operating System where some applications are installed locally and others are accessed remotely via a Server Based Computing (SBC) interface. The table below details the four scenarios where a hybrid model is likely to be an appropriate solution:

| Scenario | Description |
|---|---|
| **When applications are installed locally and also accessed via Server Based Computing scenario** | • Users primarily use applications that are installed locally on the desktop/laptop.<br>• New applications are provided via a Server Based Computing model (Discussed in section 6.1.3.1.). |
| **When the user has an accessibility requirement** | • Users may need special software installed locally which does not work on thin clients.<br>• Users may need specific hardware and hardware drivers that cannot be installed on thin client. |
| **When using Re-Purposed PC's for a Server Based Computing Scenario** | • A PC used as a thin client instead of specialist thin client hardware. This is generally used to save costs where a PC is coming to the end of its life and can be reused as a thin client.<br>• Need to continue to manage the underlying PC and operating system used to host the thin client. |
| **When the application is not compatible and requires a special platform to run** | • Users need bespoke applications that require a particular platform to run.<br>• The underlying Operating System is not compatible with particular applications so users can access these applications via a Server Based Computing scenario. |

**TABLE 19: HYBRID USE OF DESKTOP PC**

### Repurposed PCs

An organisation embarking on desktop virtualisation may also wish to re-purpose existing PCs as thin clients. For example, repurposed PCs can be used to aid a transition between thick and thin clients. Please note that these devices must have its existing data and software removed in accordance with the appropriate measures applicable to the relevant security level as set out in to the CESG Good Practice Guidelines.

The following table outlines the pros and cons of using repurposed PCs as thin client devices:

| **Pros** | **Cons** |
|---|---|
| • Reduces the overall infrastructure costs, as no special thin client devices need to be purchased.<br>• Less management and support is required for a thin client device in comparison to a traditional thick client. | • Repurposed thin client PCs require more maintenance and on-going expenses than dedicated thin client or zero client devices.<br>• Transforming a PC into a thin client requires effort as a good PC client image needs to be installed, especially if an organisation is planning to lock the device down as a dedicated thin client.<br>• As the PCs in question are generally reaching the end of their lives, issues of reliability and poorer energy consumption compared to more modern devices may need to be considered in the overall total cost of ownership.<br>• Organisation with multiple repurposed PC estate may be complex to manage. |

**TABLE 20 – PROS AND CONS OF USING REPURPOSED PCS AS THIN CLIENT DEVICES**

## Thin Client

A Thin Client is an unintelligent device which relies on other computer, usually a server for its computational roles. It is generally used to create information. A Thin Client can be used in the following ways:

### Dedicated Thin Client Machines

!

**Important Note**

There is a class of thin client, called an ultra-thin client or a zero client. Such clients do not have a full operating system: the kernel instead merely initialises the network, begins the networking protocol, connects to a server and handles the display of the server's output.

The following are typical benefits of using thin client devices:

| Area | Key Benefits |
|---|---|
| **Security** | • Thin clients typically provide greater security than thick clients because the applications and data are managed on a server located within a data centre. This centralised processing makes it easier to manage and monitor system access, and to enforce security policies and procedures so that the internal security risk is reduced.<br>• The ability to limit storage of business data locally on the thin client means that the loss of data as a result of theft will have a lower impact than is the case with thick clients.<br>• Thin clients are a good choice for organisations that must adhere to strict compliance laws, as the data is stored in the data centre and not locally on the device. |
| **Reliability** | • In the event of a natural disaster or emergency, thin clients can provide rapid business continuity because all data and applications are located within the data centre. To sustain continuity, however, an organisation would also require persistent network connectivity. |
| **Support and Management** | • Thin client devices typically have a faster deployment process in comparison to thick clients.<br>• Management of thin client devices is easier than traditional thick clients, as they can be remotely configured and managed from servers located in a data centre.<br>• Thin client devices are also less susceptible to viruses and malware, as they only access data and applications from the servers, via a web browser or remote desktop software.<br>• Thin client devices do require some management but generally have lower support costs in comparison to other devices because of the standardised nature of their hardware and operating systems. |
| **Legacy Applications** | • On thin client devices legacy applications can be redeveloped to run on other platforms. |
| **Sustainability** | • Thin client devices are energy efficient and provide significant power savings at the location they are used in comparison to equivalent thick client PCs. It could be argued that there is a power off-set in doing this as more power is required to run servers in the data centre. |

TABLE 21 – BENEFITS OF THIN CLIENT DEVICES

The following are typical limitations of using thin client devices:

| Area | Key Limitations |
|---|---|
| **Software Compatibility** | • Not all software or specialised peripherals are compatible with this approach. In particular, it may not be suitable for users with special accessibility needs. |
| **Network Connectivity** | • This model requires persistent network connection with adequate bandwidth. Slow network connection hampers users to carry out their tasks effectively. |
| **Business Continuity** | • No offline mode possible if the data centre fails. |
| **User Experience** | • This approach may not provide a thick client like experience in performance, customisation, flexibility and mobility. |

TABLE 22 - LIMITATIONS OF THIN CLIENT DEVICES

### Thin Client Using Browser

This scenario describes the scenario where a user uses a thin client (running a thin Operating System) and web based applications to connect to organisational resources through the office network. Further details about Browser / Web Services model can be found in Section 6.6.

## Laptop

The laptop as an End User Device essentially provides same functionality as a desktop but enables users to be mobile. The mobility of a laptop adds extra challenges that are discussed in this section.

The chief characteristic here is the requirement for mobility. This section will primarily concentrate on the connectivity layer, laptop and data security and the Client Side virtual application component of the presentation layer.

The table below sets out the advantages and disadvantages of mobile laptop computing:

| Pros | Cons |
|---|---|
| • Flexibility to work in the office, at home or on the move,<br>• Improved productivity by having access to services and information when required – supports flexible working patterns.<br>• Improved customer service by being able to use the information in real-time.<br>• Reduced office-space by having workforce in the field or working from home and other benefits such as, flexible working and enablement of an agile workforce. Working practices also need to be changed for a fully enabled agile workforce. | • Devices need higher levels of security than a desktop (for example disk encryption).<br>• Performance can be variable depending on network connections so ability to work offline is important.<br>• Data that was locked and physically secure in datacentres or on desktop PCs, is now held on laptops that are used in untrusted locations.<br>• Data that was accessed through trusted secure wired LAN is now also provided through shared networks such as Public Wi-Fi or mobile networks. |

TABLE 23 – PROS AND CONS OF MOBILE COMPUTING

### Laptop Security Considerations

The potential exposure of data held on laptops brings significant risks to organisations in terms of the physical security of devices, the security of data on devices and also the transmission of the sensitive information over shared and unsecured channels. The principal aim for any organisation is to secure physical and intellectual property and at the same time enable their workforce with flexible access to the information. It is beyond the scope of this document to analyse which data should reside on laptops and which data can be accessed over the unsecured channels in various government organisations.

Listed below are some basic protection goals which organisations should consider for data residing locally on the laptops and giving access to organisational data over the unsecured channels:

!

**Important Note**

The considerations below cover the basic requirements for data protection for laptop devices**.** These considerations are in addition to the normal Identity and Access Management, End Point Protection, Data loss prevention (DLP) and Information and Protection Control (IPC) that organisations should have in place to safeguard the organisations intellectual property. DLP and IPC are briefly covered in this section.

Organisations should also ensure that they comply with the relevant CESG Good Practice Guides and Policies and Standards (CESG, 2012), especially CESG good practice guides no. 4, 5 & 10 (see section 6.8). The Cabinet Office is currently undertaking a review of the Government Protective Marking Scheme. The CESG Good Practice Guides and Policies and Standards can be found at http://www.cesg.gov.uk/PolicyGuidance/Pages/index.aspx.

- Reduce the risk of compromise of information saved locally on the laptop.
- Reduce the risk of data interception during the transmission of data over the public networks.
- Ensure compliance to procedural and technical policies and standards for laptops.
- Centralised management and support (Covered in section 6.1.5.1)
- General security considerations (Covered in security section 6.5)

#### REDUCING THE RISK OF EXPOSING INFORMATION SAVED LOCALLY ON LAPTOPS

The use of laptops in enterprise environments is growing as many organisations are opting to replace their traditional desktops PC with laptops during refresh programmes. The trend is partly due to a decrease in the cost of hardware and also the growing need of mobility for the end users. Laptops offer mobility, flexibility and agility to end users but similarly put the information held on laptops at threat as the laptop can be lost or stolen.

The vast majority of government laptops have CESG approved hard disk encryption. More details can be found at:

http://www.cesg.gov.uk/publications/Documents/software_full_disk_encryption_security_characteristics.pdf.

In order to mitigate such risks and safeguard data, Mobile Data Protection (MDP) systems and procedures are needed to enable organisations to abide by regulatory and contractual requirements and comply with audits. MDP provides encryption and authentication of the data stored permanently or temporarily on local mobile devices, such as laptops, and also provides evidence that the protection is working.

**Key Consideration for Encryption Software**

Disk Encryption is a technology that converts the information on the disk into unreadable code that cannot be easily deciphered by unauthorized person. The encryption of information is achieved by use of complex algorithms. The full disk encryption software leverage hardware components such as Intel® Advanced Encryption Standard-New Instructions (AES-NI) and Trusted Platform Module (TPM) to provide highest level of disk encryption.

CESG guidance should also be referred to for Full-Disk encryption.

| Attributes | Key Considerations |
|---|---|
| **Security** | • Strong industry recognised cryptography algorithms.<br>• Use of strong encryption Key (min 128 bits) and mechanism for safe key storage.<br>• TPM and secure key storage preventing unauthorised key recovery, but allowing for key escrow. |
| **Support** | • Support for full disk encryption and encryption of removable media.<br>• Ability to encrypt drives in silent mode with minimum overall performance degradation.<br>• Multi-Platform Support across networks |
| **Performance** | • Embedded support for Intel® Advanced Encryption Standard-New Instructions (AES-NI), Trusted Platform Module (TPM) and Trusted Computing Group (TCG) standards.<br>• Integration and interoperability with current Enterprise software.<br>• A minimum encryption rate that can sufficiently support encryption activities. |

| | |
|---|---|
| | • Throttled background encryption service. |
| **Manageability** | • Centralised key management and exchange method.<br>• Ability to store encrypted keys separately from the encrypted data.<br>• Ability to centrally manage all encryption activities and provide audit and reporting capabilities.<br>• Robust support for Key Recovery for primary, remote or DR scenario. |

TABLE 24: KEY CONSIDERATIONS FOR ENCRYPTION SOFTWARE

In addition to encryption of mobile data stores (Internal Hard drives, USB Drives, External Hard drives) it is also important to safeguard organisational data throughout an infrastructure estate from malicious intent and from accidental loss. This can be done by implementing correct checks and balances and is covered further in Section 6.5.

!

**Important Note**

Organisations should also ensure that they comply with the relevant CESG Good Practice Guides and Policies and Standards (CESG, 2012). Commercial Product Assurance (CPA) is CESG's approach to gaining confidence in the security of commercial products. Assessment of products will be done against published security characteristics. More details about the assurance scheme can be found at http://www.cesg.gov.uk/servicecatalogue/CPA/Pages/CPA.aspx

### REDUCING THE RISK OF DATA INTERCEPTION OVER WIRELESS NETWORKS AND 3G

Laptops provide users with a flexible, agile way of working and enable them to remotely connect to organisational data. However, in the future these benefits will be incomplete without some dependence on wireless networks which enable mobile users to connect to Local Area Network (LAN) through a wireless radio connection via an Access Point (AP). The AP transmits the traffic between the wired and wireless part of the network by receiving and transmitting 802.11 packets.

The built-in security of the WLAN has improved with the introduction of WPA2. However, there are still instances of WLAN being compromised. The main reason for continuing issues are un-encrypted networks, use of legacy hardware, use of weak authentication protocols, use of public hotspots, lack of intrusion prevention, configuration mistakes and user training.

The security of the WLAN should be of same standard as wired LAN, despite the added complexity intrinsic to wireless networks. Intrusion prevention and vulnerability management should be at the heart of any WLAN deployment. The WLAN intrusion prevention system (WLAN IPS) monitors organisations wireless networks and mitigates risks such as man in the middle attacks, denial of service, use of unauthorised WLAN and use of unsupported WLAN technologies. The WLAN IPS capabilities can be used as an in-built capability of a WLAN products provided by WLAN vendors or for better protection a dedicated overlay capability.

A Gartner white paper (GIRARD, PESCATORE, & ZIMMERMAN, 2011) describes the risks enterprises face when implementing WLAN and how these risks can be effectively mitigated by correct use of technology, implementation of WLAN IPS security products and well defined processes.

**Key Considerations for WLAN Access Point**

The table below highlights the attributes that WLAN products should have and the key considerations against each of them.

| Attributes | Key Considerations |
|---|---|
| **Security** | • Ability to provide WLAN Intrusion and Prevention and Detection for dedicated security overlay to prevent organisational resources from:<br>▪ Denial of Service<br>▪ Man in the Middle Attack<br>▪ MAC Spoofing<br>▪ Network injection<br>• Ability to support strong encryption algorithms |
| **Support** | • Radio Frequency (RF) interference mitigation<br>• Prior site survey and testing to provide good coverage<br>• Minimum support of WPA2 |
| **Performance** | • Ability to perform uniform upload and download performance (If required). |
| **Manageability** | • Ability to provide vulnerability management<br>• Ability to monitor WLAN infrastructure health<br>• Solution that seamlessly integrates with other networking devices from same or different vendor |

TABLE 25: KEY CONSIDERATIONS FOR WLAN ACCESS POINT

### CONSIDERATIONS WHEN USING WI-FI AT PUBLIC PLACE

Free to use Wi-Fi access points are everywhere, with even some local councils providing Wi-Fi access throughout cities. This expansion allows laptops and mobile devices to establish an internet connection with a press of a button and remain connected by hopping from one access point to another by re-establishing the connection.

This readily available technology is good for occasional internet browsing on a personal device, however, there are some potentially serious security implications if public Wi-Fi is used on corporate laptops for connecting to corporate resources. Many Wi-Fi access points are left open with no encryption key, leaving devices connecting to Wi-Fi wide open to attack. Threats may include:

- Packet sniffing software which is easily available to hackers allowing them access to the data on someone else's computer via a Wi-Fi network.
- Threats where hackers access information on the computer, and can "insert themselves" into the network to launch man-in-the-middle attacks.
- Malicious devices broadcasting itself as an access point and tapping all the information that is transmitting from a person's computer.

Free Wi-Fi can be safely used to connect to corporate networks by having correct set of tools, providing end-to-end security for example encryption. This list of tools and best practice detailed below minimises the risk but does not completely eliminate it.

- Users should connect to corporate resources via VPN (Virtual Private Networks) or similar encryption protocols.
- Connection to browser enabled applications should be via an SSL interface.
- Industry approved Intrusion Prevention and Detection software should be installed on laptops.
- Up-to-date antivirus software should be installed and enabled on laptops.
- A personal firewall correctly should be configured and enabled on the laptop.
- Full disk encryption should be enabled on the laptop device.
- Operating System should be up-to-date with security patches.

### Ensuring compliance and adherence to physical security standards for laptops

The physical security of a laptop is generally the responsibility of the individual who is allocated the business laptop. It should be the organisation's responsibility to provide reasonable means by which an individual can secure their business laptop.

## Tablets and Smartphones

A tablet is a mobile computer that runs on an adapted version of Operating System. It has a touch screen or a pen enabled interface. A tablet is generally used to consume information e.g. reading emails or documents, browsing the web. API's (Application Programming Interfaces) on a tablet allows third party applications to have good integration with OS (Operating System) and underlying hardware and provide a rich user experience.

A Smartphone is a mobile device built on a mobile platform with greater computing power and connectivity options than a traditional feature phone. Smartphones generally include high resolution touch screens and web browser. The underlying experience may be very similar to a tablet device limited only by the size of the screen.

## Current Market Landscape

Mobile and tablet devices are likely to be used as secondary supporting device by users to perform activities such as viewing e-mails, documents and messages. The major limitation on use is the lack of a physical keyboard and mouse which most users find essential for prolonged use particularly when creating information. Using these devices helps employees to stay synchronised with their colleagues irrespective of their physical location. With increasing costs of travel and commuting, many organisations are promoting remote-access policies in order to improve employee productivity. While smartphones are not yet replacing the role of stand-alone computers, the emergence of tablets haves taken the capabilities of mobile devices' to a new level and tablet functionality is likely to improve further with time. Mobile operating systems will also continue to evolve to enable consumers and business users to do more with a mobile device.

### Smartphone / Tablet Device Provisioning Models

There are many enterprise models for implementing a mobile device management framework. Three of the key models are assessed in this section.

**Individual Liable Model / BYOD:** Employees buy their own devices and decide which applications to run on them. Employer pays a fixed amount of reimbursement towards their employees mobile spend. This type of model falls under Bring Your Own Device (BYOD) category.

**Corporate Liable Centralised Model:** The organisation provides device and calling plans which have corporate discount. All the phones and numbers are owned by organisation and consolidated billing is managed centrally.

**Mixed model (Corporate model with BYOD):** Organisation provides a device (and calling plan for smartphones) for selected employees, whilst others use their own devices for work. The organisation may or may not reimburse the expenses towards device spend but implements security policy for devices connecting to enterprise network. If an organisation is considering a mixed model, then they should carefully assess the existing compliance legislation.

The table below shows comparison across all three mobile device management models.

| Model | Pros | Cons |
|---|---|---|

| | | |
|---|---|---|
| **Individual Liable Model** | • Can be low costs for employer as some expense is automatically passed on to employee.<br>• Low accounting and IT headache as refresh and choice of device are the responsibility of the user and this is cheaper from an IT perspective | • Not permitted under current GSI code of connection – there is currently no CESG approved model for BYOD devices.<br>• Implementing security across the enterprise for all types of devices can be difficult.<br>• Security breaches are difficult to detect.<br>• Device policies cannot be enforced 100% as some employees will install personal preferences. |
| **Corporate Liable Model** | • Corporate discounts and plans save costs for employees.<br>• As devices are owned by company, risks are mitigated considerably.<br>• Tracking of wireless units and centralised payment streamlines the process.<br>• Security and usage policies can be implemented stringently. | • Device replacement cost is considerably high compared to buying a new device.<br>• Possible misuse of mobile devices for personal usage. |
| **Mixed Model** | • Flexibility and ample choice between applying individual or corporate liability model. | • Can cause procedural problems when it comes to administration.<br>• Policy implementation across the enterprise is still complicated especially when interfacing between devices owned by employer and those owned by employees. |

TABLE 26 - COMPARISON OF MOBILE DEVICE PROVISIONING MODELS

!

**Important Note**

The assumption for the above table is that government organisations would have moved to new GPMS security levels.

### Mobile and Tablet Web Applications

Web applications for mobile devices are different to the applications used on stand-alone systems such as laptops. This is because smartphones have a limited capacity and applications therefore need to be relatively small. While the arrival of tablet computers and high-performance smartphones is altering this picture, as many devices are now capable of handling complex programs and data processing, it is still imperative that mobile applications remain accessible from lower-end smartphones. To address issues related to mobile device compatibility, W3C and Mobile Best Practices Working Group have proposed guidelines for implementing browser based applications for mobile devices. The document is an open standard (W3, 2012)

A useful tool for checking a website's compatibility with mobile device standards is the web-based extension of the 'MobileOK' scheme. MobileOK is designed to improve the web experience for users of mobile devices by rewarding content providers that adhere to good practices when delivering content to them. It does not interfere with non-mobile devices and does not imply endorsements or suitability of content. Another software package called 'checker' has been designed to provide automated checking of conformance. The tool is free and can be accessed at http://validator.w3.org/mobile/?docAddr=http%3A//www.w3.org/Mobile/.

## 6.2 Implementation Guidelines

This section of the Framework provides specific implementation guidelines around the various technology solutions identified. It provides key considerations for government organisations when deploying, upgrading or maintaining their Information Communication and Technology (ICT) environment.

The implementation guidelines cover the following specific solutions:

- Desktop with Thick OS
- Thin Client with Thin OS
- Laptop with Thick OS
- Tablet / Smart Phone with Mobile OS

The high-level guidelines in this section are focused on specific technologies rather than individual proprietary components which may be part of an overall solution. The guide provides key information which can form the basis of decisions when considering solutions for a particular user segment. The implementation guidelines provide a framework for proprietary as well as Open Source components.

### 6.2.1 Desktop with Thick OS

This section will detail the guidelines for implementing desktop PC with Thick OS. Refer to section 6.1.4 for definition of Thick OS and section 6.1.5.2 for definition of Desktop.

#### 6.2.1.1 Desktop Hardware Considerations

The Government's strategic goals outline a preference for a desktop device that uses mainstream technologies, is readily available in the market and is compatible with technologies that are foreseen to be available in near future.

| Attribute | Key Considerations |
|---|---|
| **Virtualisation** | • Desktop hardware should be compatible with virtualisation technologies including client side virtualisation where appropriate. |
| **Encryption** | • Desktop hardware should support full disk encryption where required. |
| **User Experience** | • Desktop hardware should be compatible with and supports server based computing without adversely affecting user experiences. |
| **Wi-Fi** | • If required, desktop hardware that supports IEEE 802.11n standards should be considered. |
| **Physical Security** | • Provided by locked down premises. Also ability to lock the devices to desks, for example, with locks. |
| **Biometric Authentication** | • If required, compatible hardware to support Biometric Authentication should be considered. |
| **Accessibility** | • There should be special consideration for desktop hardware that supports requirements for users with accessibility issues. |

| | |
|---|---|
| **Support and Maintenance** | • Consider carefully the level of support required – this will differ for different groups of users and roles. For some a move to a self-service model may be appropriate. |
| **Operational Service** | • Consider what service levels are acceptable. Higher service levels will clearly incur greater costs over the lifetime of the device. |

TABLE 27 - KEY CONSIDERATIONS FOR DESKTOPS

### 6.2.1.2 Device Management Considerations

The organisation needs to determine the optimum support model and decide whether it is appropriate for some groups of users to self-support. For those groups where it is not appropriate desktop management is a fundamental part of user environment management and achieving a well-managed, locked down desktop environment will provide considerable savings both in terms of TCO and day-to-day operational costs.

The table below sets out best practice for a range of key attributes:

| Attribute | Key Considerations |
|---|---|
| **OS Deployment** | • A centralised deployment platform that allows IT administrators to fully deploy and configure desktop, laptops, servers and other mobile devices from bare-metal deployment. The deployment includes a centrally managed image of the OS and core applications that are common to all users. |
| **Application Deployment** | • A centralised distribution of software to devices that are across multiple complex networks. Target computers are generally identified automatically and applications are installed in silent mode. |
| **Patch Management** | • A centralised system for software update management where updates can be pushed and deployed to the operating system, third-party applications, and line-of-business applications on any end user device. |
| **Anti-Virus (AV) and Firewall Management** | • A centralised management for AV installation**,** reporting and updates for all devices. AV management includes mechanisms for checking that machines have an up-to-date service engine and definition files. A mechanism to centrally manage Firewall configuration and Policies for Laptops and Desktop devices |
| **Hardware and Software Inventory** | • A centralised capability to record and track the hardware and software assets held by an organisation, coupled with management reporting functionality to provide a current “as-is” view of organisational assets. |
| **Monitoring and Remediation** | • A centralised monitoring system that shows the state, health and performance information of the various computer systems operating in an organisation. When errors are detected, the system raises alerts and notifies other relevant systems. The monitoring and remediation systems can also automatically remediate common and mundane issues that are resolved generally by rebooting a device or restarting a service. |
| **User Rights on local Machine / OS Lockdown** | • A centralised system that pushes locked down user and computer settings to devices and periodically checks that the intended configuration still exists. |
| **Processes and Policies** | • Policies and procedures that govern how Information, Communication and Technology (ICT) are consumed within an organisation. Well written |

| | |
|---|---|
| | and clear policies help users to benefit from the ICT as intended by an organisation. Also, policies help users understand their responsibilities and eliminate any ambiguity that might lead to potential security risks and user frustration. |
| **Integration with Configuration Management Database (CMDB)** | • A CMDB is a database containing information about the components used in an organisation's IT system and the relationships between the components. Each component in CMDB database (such as hardware, software, documentation, and personnel) is referred as configuration item (CI). Configuration management seeks to specify, control, and track configuration items and any changes made to them in a comprehensive and systematic fashion. |
| **User State Virtualisation (USV)** | • USV is a process by which a user's personal settings, documents and software components are made independent of the underlying hardware and applications. This allows users to log-on to different devices from different locations and user's experience same personalised environment. The personalised user attributes are saved centrally and during log-on are delivered directly to the user's desktop (virtual or local), laptop or a similar end user device. |

**TABLE 28 –A WELL MANAGED DESKTOP ENVIRONMENT**

#### 6.2.1.3 Desktop Connectivity Considerations

Desktops are fixed in one location and have permanent network connectivity using the Local Area Network (LAN). The desktop may also be compatible with Secure Wi-Fi (if required). Most of the desktop solutions support off-line working using local or cached applications and user profile in the event of network failure. However, a desktop is dependent on permanent (LAN) connectivity in order to provide following functionalities:

- Connection to centralised database for real time user authentication, authorisation and identity.
- Access to centrally stored core user attributes such as user profile, user documents and personalised application settings.
- Access to shared drives and central repositories for collaboration.
- Access to applications that are hosted remotely in a datacentre or where an application is deployed in typical client / server architecture.

#### 6.2.1.4 Desktop Application Considerations

The applications can be presented locally or remotely to a desktop device. Due consideration should be given in each case:

| Attribute | Key Considerations |
|---|---|

| | |
|---|---|
| **Local Computing** | • Adequate resources available to run applications that are installed locally.<br>• The dependency on persistent network connection is not required unless data is not held locally. Users can be productive during network failure and work offline.<br>• There is a high dependency on local hardware availability.<br>• Generally high support and maintenance costs are associated with de-centralised applications.<br>• Bespoke, proprietary or in-house applications that are sometimes written in such a way that they are dependent on OS version or underlying hardware. |
| **Remote Computing** | • Minimum local computing resource required.<br>• There is a high dependency on persistent network connection. A network failure will result in a loss of application services.<br>• There is a high dependency on data centre availability (Remote Access Service).<br>• Further demand on available bandwidth.<br>• Generally lower support and maintenance costs are associated with centralised applications.<br>• Applications that are remotely presented are independent of local hardware or software attributes. For example, applications presented via a browser or applications only requiring Server Based Computing Receiver on local desktop. |

TABLE 29 – KEY CONSIDERATIONS FOR APPLICATIONS

### 6.2.2 Thin Client with Thin OS

This section will detail the guidelines for implementing Thin Client with Thin OS. Refer to section 6.1.4 for definition of Thin OS and section 6.1.5.2 for definition of Thin Client.

#### 6.2.2.1 Thin Client Hardware Considerations

The list below provides best practice for a thin client device.

| Attribute | Key Considerations |
|---|---|
| **Virtualisation** | • Client Side – A thin client that is compatible with virtualisation technologies like Server Based Computing. This means that the thin client software (firmware) should have all the necessary protocols and software clients that support open standards. For larger Hosted Virtual Desktop environments, thin clients should also support the respective connection broker that assigns the correct virtual desktops to the respective end devices.<br>• Server Side –The data and applications reside on the servers in the data centre. The servers should therefore be dimensioned so that in the event of the failure of one server, the other remaining servers can take on the added workload. |
| **User Experience** | • A thin client that is compatible and supports server based computing without adversely affecting user experiences. Also, check whether the thin client is capable of delivering a rich multimedia experience at the endpoint. |
| **Accessibility** | • There should be special consideration for thin client hardware that supports requirements for users with accessibility issues. |

**TABLE 30 – KEY HARDWARE CONSIDERATIONS FOR THIN CLIENTS**

!

**Important Note**

Doing a proper holistic business impact assessment including that of networks, servers, user training etc. is imperative before considering thin clients.

**<u>Key Considerations For Using Repurposed Pcs As Thin Clients</u>**

The following are some key considerations for organisations thinking about using repurposed PCs as thin client devices:

- Prior to the start of a desktop virtualisation project, an organisation should decide on the cut-off age of old PCs to be repurposed as thin clients and evaluate the costs for doing so.
- It is advisable that PCs more than 3 years old are repurposed as thin clients provided they are in good state.

- Depending on how organisations use a repurposed PC, they may still need to license an operating system, antivirus product, management tool and manage updates on the client device.
- TCO needs to consider reliability and energy efficiency.

## Key Considerations for Infrastructure Requirements

The following are the key infrastructure considerations in a server-hosted environment:

**Server Requirements** – The system CPU and memory requirements may be calculated using a specific vendor's reference architecture or sizing guideline. Memory (RAM) requirements are straightforward to calculate utilising vendor supplied sizing information.

**Storage Requirements** – Server Based Computing can have a significant impact on storage. Storage can also play a significant role in the overall performance of the Desktop & Application Publishing and Hosted Virtual Desktop solutions. It is therefore important to understand the storage capacity requirements.

### 6.2.2.2 Thin Client Management Considerations

Thin client device management is a fundamental part of user environment management and achieving a well-managed environment will provide considerable saving both in terms of TCO and day to day Operational costs. Thin client devices are easier to manage as compared to traditional thick clients, as they can be remotely configured and managed from servers located in the data centre. The technology itself is based on a Server Based Computing platform that centralises endpoint images as virtual machines, such that the endpoint device only runs a thin client OS that is consistent across all similar devices. When needed, IT staff can quickly add or patch applications from the data centre, and the next time the users accesses their image the applications and operating systems are in full corporate compliance without the need to push an update.

OS deployment, Patch management and other attributes of a well-managed desktop environment are relevant to thin clients as well and have already been discussed in Section 6.1.5.2.

### 6.2.2.3 Thin Client Connectivity Considerations

Thin client devices are fixed in one location and have permanent network connectivity using the Local Area Network (LAN). Thin client devices do not support off-line working. They are primarily dependent on permanent (LAN) connectivity in order to provide following functionalities:

- Connection to centralised database for real time user authentication, authorisation and identity.
- Access to centrally stored core user attributes such as user profile, user documents and personalised application settings.
- Access to shared drives and central repositories for collaboration.
- Access to applications that are hosted remotely in datacentre.

- Provide support for the bandwidth hungry peripheral devices.

**Network Requirements** – It is important to consider the networking requirements, both between the servers and clients running Hosted Virtual Desktop or Server Based Computing receiver, along with internal server to server networks and storage networks. All these networks should be configured properly as networking requirements can vary significantly, depending primarily upon the size of the server used to host the Desktop & Application Publishing or Hosted Virtual Desktop sessions. The overall user experience is highly dependent on a reliable network with sufficient capacity to cope with peaks in demand.

#### 6.2.2.4 Thin Client Application Considerations

Applications are presented remotely to a thin client device. Some of the factors to guide choice are:

| Attribute | Key Considerations |
|---|---|
| **Local Computing** | • Generally, thin client is a non-intelligent terminal and hence does not perform any computing tasks locally. |
| **Remote Computing** | • Minimum local computing resource required.<br>• High dependency on persistent network connection. A network failure will result in unproductive users.<br>• High dependency on data centre availability.<br>• Generally lower support and maintenance cost associated with centralised applications.<br>• Applications that are remotely presented are independent of local hardware or software attributes, for example: application presented via a browser or application only requiring Server Based Computing Receiver on local thin client device. |
| **Resource Intensive Applications** | • Intensive applications, such as video streaming, multimedia and 3D interface, need special consideration. Thin clients are typically good for traditional business or process applications, but may not be appropriate for intensive applications. |

TABLE 31 – KEY CONSIDERATIONS FOR APPLICATIONS

### 6.2.3 Laptop with Thick OS

This section will detail the guidelines for implementing Laptop PC with Thick OS. Refer to section 6.1.4 for definition of Thick OS and section 6.1.5.2 for definition of Laptop.

#### 6.2.3.1 Laptop Hardware Considerations

The list below provides key laptop hardware considerations.

| Attribute | Key Considerations |
|---|---|
| **Virtualisation** | • A laptop hardware that is compatible with virtualisation technologies where technology such as Client Side Virtualisation is considered. |
| **Encryption** | • A laptop hardware that supports full disk encryption and password on boot technologies and supports TPM chips. |
| **User Experience** | • Laptop hardware that is light in weight, easy to carry on and supports Server Based Computing without adversely affecting user experiences. |
| **Wi-Fi** | • Laptop hardware that supports IEEE 802.11n standards |
| **Physical Security** | • Laptops with T-Bar or similar lock. |
| **Biometric Authentication** | • If required, compatible hardware to support Biometric Authentication. This is build-in on most laptops as standard. |
| **Accessibility** | • There should be special consideration for laptop hardware that supports requirements for users with accessibility issues. |

TABLE 32 – KEY CONSIDERATIONS FOR LAPTOPS

#### 6.2.3.2 Laptop Management considerations

Laptop management is a fundamental part of user environment management and achieving a well-managed, locked down laptop environment can provide considerable savings both in terms of total cost of ownership (TCO) and day-to-day operational costs.

This area is covered in section 6.1.5.2 and is relevant to laptops as well. However, when laptops are used in the field authentication provides challenges.

| Attribute | Key Considerations |
|---|---|
| **Laptop Authentication** | The authentication process of laptop is same as desktop when the laptop is on LAN and authentication is provided by centralised directory system. However, when the laptop is in field the user will generally authenticate locally via a cached profile and then connect to the organisational resources via a secure channel, the authentication and authorisation is checked by central systems before the laptop is allowed to make connection. Use of multi-factor authentication such as use of tokens can further improve security and reduce risks. |

TABLE 33: LAPTOP MANAGEMENT CONSIDERATIONS

#### 6.2.3.3 Laptop Connectivity Considerations

Laptops are often the primary mobile devices used by Mobile Knowledge workers from a variety of locations including home offices, untrusted public locations and trusted office locations. Laptops can connect to organisational resources from wired LAN, wireless LAN, 3G / GPRS data cards, public WI-FI and Wi-Fi from a home office. A laptop provides self-contained environment where users can work and create content locally that can be synchronised with the central database when connection is available. The following persistent connectivity considerations are key:

- Remote connection to centralised database for user authentication, authorisation and identity.
- Remote access and synchronisation of centrally stored core user attributes such as a user's profile, documents and personalised application settings.
- Remote access to shared drives and central repositories for collaboration.
- Remote access to applications that are hosted remotely in datacentre or where an application is deployed in a typical client / server architecture.
- Extensive use of VPN and encryption protocols to safeguard data integrity and confidentiality.

#### 6.2.3.4 Laptop Application Considerations

Applications on laptop devices can be presented locally or remotely. Some of the factors to guide choice are:

| **Attribute** | **Key Considerations** |
|---|---|
| **Local Computing** | • Adequate resources should be available to run applications that are installed locally.<br>• The dependency on persistent network connection is not required unless data is not held locally. Users can be productive during network failure and work offline.<br>• There is a high dependency on local hardware availability.<br>• Generally high support and maintenance costs are associated with de-centralised applications.<br>• Bespoke, proprietary or in-house applications that are sometimes written in such a way that they are dependent on OS version or underlying hardware. |
| **Remote Computing** | • Minimum local computing resources are required.<br>• There is a high dependency on persistent and secure network connections. A network failure will result in unproductive users.<br>• There is a high dependency on data centre availability.<br>• Generally lower support and maintenance cost are associated with centralised applications.<br>• Applications that are remotely presented are independent of local hardware or software attributes, for example, applications presented |

| | |
|---|---|
| | via a browser or application only requiring Server Based Computing Receiver on local desktop. |

TABLE 34 – KEY CONSIDERATIONS FOR APPLICATIONS

Particular thought needs to be given to the presentation of basic applications such as word processing. One key advantage of a laptop lies in the ability to work offline if a network connection is unavailable. Best practice implementations will not preclude that option.

### 6.2.4 Smartphone / Tablet

This section will detail the guidelines for implementing Smartphone / Tablet with Mobile OS. Refer to section 6.1.4 for definition of Mobile OS and section 6.1.5.2 for definition of Tablet / Smartphone.

#### 6.2.4.1 Tablet / Smartphone Hardware Considerations

| Attribute | Key Considerations |
|---|---|
| **Virtualisation** | • Not applicable. |
| **Encryption** | • A mobile hardware that supports encryption should be selected. |
| **User Experience** | • Generally, a user's experience will be richer on a tablet in comparison to a smartphone. The user's experience also depends on content and service provided. If applications rendered on handheld devices are written and tested with smartphones and tablets in mind, then the end user experience will be richer.<br>• In comparison to desktops and laptops, users may have limited functionality on mobile devices and the overall experience will be different. |
| **Wi-Fi** | • Mobile device supports IEEE 802.11n standards. |
| **Physical Security** | • Not applicable. |
| **Biometric Authentication** | • If required, the selected devices should be compatible hardware to support Biometric Authentication. |
| **Accessibility** | • The devices should be able to access organisation's business applications like emails etc. There should be special considerations for mobile hardware that supports requirements for users with accessibility issues. |

TABLE 35 – KEY CONSIDERATIONS FOR TABLET / SMARTPHONE

#### 6.2.4.2 Tablet / Smartphone Management considerations

Tablet and smartphone management is a fundamental part of user environment management. In some cases a single instance of device management software is able to manage desktops, laptops and servers, as well as mobile devices but there are a number of niche suppliers who specialise in particular devices or operating systems.

The management software chosen for the management of mobile devices should be capable of securing, recovering or wiping data remotely on mobile devices as well as having a built in capability for the Identity Assurance. Alternative approaches would be to use mobile devices to allow users securely connect to the data and not allow any data or configuration to be stored directly onto the mobile device. This approach minimises the dependency on management software but limits the use of devices and increases reliability on authorisation, authentication and integrity systems.

#### 6.2.4.3 Tablet / Smartphone Application Considerations

Applications can be presented locally or remotely to devices. Due consideration should be given in each of the following cases:

| Attribute | Key Considerations |
|---|---|
| **Local Computing** | • The Client Side interface of the business application runs as an app on the mobile devices and connects to the back end service.<br>• A local app may provide a very good user experience but relies on the native capabilities of the device – different versions of the app may be required for different devices.<br>• There is a high dependency on local hardware availability.<br>• Applications may depend on browser compatibility which may vary across devices. |
| **Remote Computing** | • Many virtualised apps cannot take full advantage of the modern features of a touchscreen device and therefore provide a poorer user experience.<br>• There is a high dependency on a persistent and secure network connection. A network failure will result in unproductive users.<br>• There is a high dependency on datacentre availability. |

**TABLE 36 – KEY CONSIDERATIONS FOR APPLICATIONS**

## 6.3 Open Source Considerations

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

The following set of documents currently make up that toolkit:

- All About Open Source – including FAQs
- ICT Advice Note - Procurement of Open Source
- Procurement Policy Note on Open Source
- OSS Options
- CESG Guidance on Open Source - for Government users only
- Publically accessible summary of the security guidance
- Total Cost of Ownership
- Total cost of ownership of open source software: a report by the London School of Economics for the UK Cabinet Office supported by OpenForum Europe
- All about Open Source – new appendices available (2012 update)
- OSS Options – new entries added (2012 update)
- Total Cost of Ownership – more detail to assist in the calculation of TCO (2012 update)

## 6.4 Accessibility Considerations

Around 18% of the UK population has a disability as defined by the Equality Act (formerly the Disability Discrimination Act) i.e. a physical or mental impairment that has a substantial and long-term adverse effect on their ability to perform normal day-to-day activities. The law requires organisations (including Civil Service departments) to make systems and services accessible to these users or to provide reasonable adjustments.

The Civil Service is required to employ a workforce that is representative of the population it serves, and departments have disabled staff e.g. around half of all HMRC staff have completed their diversity declaration and, of these, 15% have recorded that they have a disability. The percentage of Civil Service Staff with accessibility needs is more likely to increase rather than decrease. Disability rates increase with age and HMRC, like many departments, has an 'aging' workforce.

ICT can be difficult to use for many disabled staff e.g. those with a visual impairment, motor impairment (RSI, arthritis etc.), dyslexia or hearing impairment. Specialist hardware or software (for e.g. screen readers, voice activation etc.) can be provided as reasonable adjustments. Some staff members have issues but do not consider themselves to be 'disabled'. Others have issues (e.g. eyesight difficulties, some wrist or hand problems) below the level set by the legal definition, but still have problems using equipment. Display Screen Equipment (DSE) assessments for example can recommend ergonomic keyboards and mice that are designed to stop conditions arising or getting worse. In short, getting the right equipment is important for potentially any member of staff and not just those who are 'disabled'.

!

**Important Note**

Legal Definition of Disability - The Equality Act generally defines a disabled person as someone who has a mental or physical impairment that has a substantial and long-term adverse effect on the person's ability to carry out normal day-to-day activities. This differs slightly from the definition in the DDA, which also required the disabled person to show that an adversely affected normal day-to-day activity involved one of a list of capacities such as mobility, speech, or hearing. Source: http://odi.dwp.gov.uk/disabled-people-and-legislation/equality-act-2010-and-dda-1995.php

DSE - Display Screen Equipment Regulations in UK laws cover the need to ensure employees have their PCs, chairs, desks etc. correctly positioned. If employees have any problem then staff trained as DSE can recommend a range of solutions e.g. some ergonomic mice.

### 6.4.1 Major Accessibility Needs

From an End User Device perspective, departments must provide staff with equipment that allows them to carry out their duties safely and effectively. The law does not require that all products must be usable by all staff. As a starting point, this strategy envisages that all applications and systems (etc.) should at least be available to staff via a desktop or laptop PC, as appropriate to their business needs.

Currently the majority of specialist products have been written to work on Windows based PCs (e.g. drivers for some ergonomic keyboards, software like Dragon that requires increased processing power). Following this strategy means that, as a worse case, disabled users can be guaranteed that any solution for them now in place will continue in the future and will not be disadvantaged. However, it also allows for the possibility that access to a wider range of devices might in itself offer better solutions for some staff than are currently available. Some of these possibilities are covered in Section 6.4.2.

Please note that some disabled staff members are allowed to work from home as a reasonable adjustment, so 'access to applications, systems etc., via a desktop or laptop' in this context can also include remote connectivity for some users (plus a printer in some cases).

### 6.4.2 Accessibility Technology Considerations

Once a user's needs are identified, specific technology can be used to improve usability if required. The following considerations will aid in decision making process when choosing this technology:

- Technology that helps disabled users to achieve their day to day tasks as comfortably and as efficiently as possible.
- Technology that allows disabled users to efficiently use EUD devices and applications in timely manner.
- Technology that avoids unintentional activation of controls and be able to provide equivalent security and privacy as an able user.
- Technology that is easy to use and requires minimum training and where accessible training and support materials are available.
- Technology products that are developed according to ISO/IEC guidelines.

#### 6.4.2.1 Accessibility Considerations for Browser Enabled Applications and Thin Clients

Applications presented through a browser should be built to WCAG AA standards (Europa, 2011). Currently the Government mandates WCAG v1 AA for customer facing sites, but WCAG v2 AA is also acceptable. The standard is aimed at Internet hosted systems but can be applied equally to those systems provided to staff via an Intranet. Usability is also important to disabled people – if using a mouse is difficult it is clearly important to be able to complete a transaction with the minimum number of mouse clicks. BS8878 provides a good basis for application design.

[Not all applications (including word documents, web applications etc.) are of course presented through a browser, some are installed locally on devices. There is an ISO accessibility standard covering such systems though it is out of date, and a new set of standards is being produced in the EC (Mandate 376). Similarly, WCAG does not apply to Word documents, spread sheets, PDFs etc. Users can be disadvantaged when a system they are presented with is accessible but the user guide is not. Organisations may therefore have their own standards for these areas].

Applications and other software tools built to standards may still not be accessible, in that some users will need specialist hardware or software to drive their machines and hence gain access to these applications. 'Thin Client' devices that principally support access to applications presented through a browser tend to be low powered and therefore may not support products such as text to speech converters, which typically need increased processor power. Similarly, Thin Client operating systems may not support drivers for specialist hardware or any software tools (e.g. for calibration) these hardware items require. On the other hand, it is possible that some Thin Client devices may have accessibility functionality built into them such as magnification, colour change or narration (text to voice), and may allow menu text styles and sizes, icon sizes to be easily changed. These features may be of use to users with mild to moderate visual impairment or dyslexia (or related conditions). In some circumstances, it is possible that these solutions may be preferable to a traditional PC with additional specialist software.

#### 6.4.2.2 Accessibility Considerations for Handheld Devices

Devices in this category may include tablets. In some situations these handheld devices may be considered to be portable thin client devices, and the considerations above apply – lower powered tablets may not be capable of running the specialist tools some disabled users need. However they may offer advantages to some users:

- Their lightweight design may be of use to staff members, who have issues carrying the weight and bulk of a laptop.
- Some devices have accessibility features built in including magnification, colour change, narration, menu text and icon size change etc. As mentioned above, these may be of potential use to some visually impaired staff, and those with dyslexia or related conditions. Similarly the use of a built in camera plus OCR software plus text to voice may be of use to any of these staff where they need to read printed text as part of their duties.
- Products like the iPad may also allow very basic voice activation (e.g. a cut down version of Dragon) which may help some staff with mild to moderate motor impairment (e.g. RSI, arthritis). Similarly, a touchscreen may also be of benefit to some users who have difficulty using a mouse for example.

#### 6.4.2.3 Accessibility Considerations for Smartphones

Devices in this category can be thought of, from an accessibility perspective, as mobile phones with large touchscreens plus applications that run on operating system such as iOS and Android, and hence can access web based systems. Generally they are likely to be difficult to use by many staff with disabilities, for example the small screen size could be problematic for staff with visual impairment or even poor eyesight. The touchscreen and small buttons can be difficult for those with dexterity issues though they may be of benefit to some disabled users. Many now come with text to voice in built so that they can read menu options, mail and messages, web page content etc., aloud. They are very portable of course and camera / OCR / text to voice tools are available on the market. Touchscreens (and handwriting recognition software for use with a touchscreen) may be of benefit to some staff with motor impairment.

#### 6.4.2.4 ACCESSIBILITY CONSIDERATIONS FOR BRING YOUR OWN DEVICE

Disabled staff may have personal PCs (or other devices) set up to suit their needs, with tools they have become familiar using and maintaining. If they were able to use these devices for work purposes, and if the systems they use in this context were built to standards, they may prefer to do so – they may find them more comfortable and easy to use than devices provided through work, and may have more confidence and practical experience in the tools they choose to use.

## 6.5 Security

This section currently describes best practice in relation to security. The EUD programme is working closely with key stakeholders to define the appropriate technical controls in line with the new model envisaged by the review of the Government Protective Marking Scheme and will produce detailed guidance in the next iteration of this framework.

Devices are often seen as the first line of defence in ICT environments. Most user activities will be performed on devices as will most users' interaction with possible sources of threat. The central government's risk avoidance approach provides an opportunity to leverage new enabling technologies. This section outlines a suggested approach to enable use of devices in line with the emerging strategy for the new Government Protective Marking Scheme.

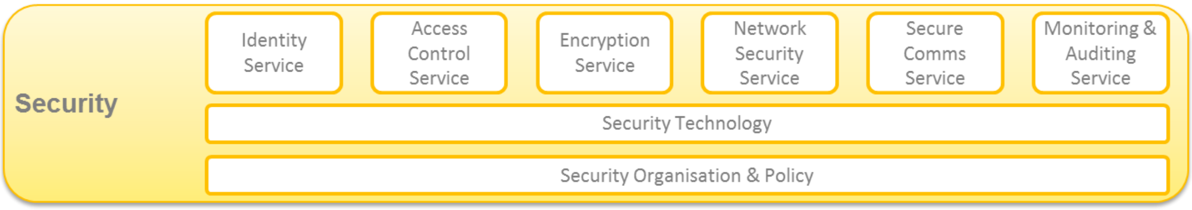


**FIGURE 5 - SECURITY SERVICES**

This section is not an attempt at creating a security model and any organisation going down the route of enabling staff with latest mobile infrastructure should perform appropriate risk management activities, including understanding the relevant:

- Threat sources and actors
- Value of assets
- Vulnerabilities
- Impact of loss or compromise

Similarly the guidance and discussion about end-user devices found below should not replace sound product selection analysis including the development of a thorough business case.

Organisations should also ensure that they take appropriate notice of the relevant CESG Policies, Standards and Architectural Patterns (CESG, 2012), especially CESG good practice guides no. 23, 24 & 28, the CESG Architectural Patterns, especially Mobile_Remote_End_Point_Devices and the CESG paper Platforms Secure by Default (see section 6.8), CPNI standards, ISO/IEC 27001 standards and with the Identity Assurance requirements of the Public Services Network (PSN) and G-Cloud programmes. The Cabinet Office is currently undertaking a review of the Government Protective Marking Scheme.

!

**Important Note**

CESG is the UK Government's National Technical Authority for Information Assurance (IA) and protects country's vital interests by providing policy and assistance on the security of communications and electronic data. More details can be found at http://www.cesg.gov.uk/AboutUs/Pages/aboutusindex.aspx.

PSN's objective is to see users seamlessly linked through a 'network of networks', governed by uniform standards and capable of accessing a range of business services when they need them with security and integrity guaranteed.

### 6.5.1 Objectives

The following outlines some of the main principles behind the security architecture in the EUD Framework. These need to be considered alongside policies and guidance published by CESG and by the PSN and G-Cloud programmes. Consideration should also be given to the expected changes under the Government Protective Marking Scheme Review.

### 6.5.2 Defence in depth

Defence in depth as a general principle has two high level impacts of the configuration and design of the end-point. First of all it is vital that an end-user device type does not become the weak link of the (security) chain. This means ensuring that it is controlled from a security point of view. The second aspect is that in order for the defence in depth approach to be effective it needs to leverage security controls implemented at other layers, e.g. using authentication mechanisms at a central access point.

The End User Device Framework outlines a number of security services that applies to all end-user devices. Some, will require implementation on the device others need central Security Enforcement Points.

### 6.5.3 Security Services

The following sections discuss the relevant security services from the EUD Framework in the context of devices like desktops, laptops, thin clients and mobiles. It is important to keep in mind the overall governance of security. The secure use of the devices will be driven by the organisations approach to risk management.  Risk management is a top down approach and should be performed on all systems, including on all devices and their usage and residual risks need to be managed in alignment with Government processes. These processes should include proper monitoring and auditing of the effectiveness of controls (whether procedural or technical).

#### 6.5.3.1 Identity services

A fundamental security objective in the implementation of the Government's ICT Strategy is that any action with a certain impact level can be tied to the individual performing it. Identity management is the fundamental building block to achieve this (with access control and auditing also constituting other important elements). Identity should fundamentally be managed once, since managing the different identities in Government on a device level is not practical. What may differ is the approach for a user to authenticate themselves against the services that they use. The method to do so can vary but this has no impact on how identity is managed. This section should be read in conjunction with the good practice guides, policies and guidelines published by CESG (CESG, 2012) and the Identity Assurance guidance from the PSN and G-Cloud programmes.

## Identity Services At Device Level

Different approaches exist to ensure a user is who they say they are. Depending on the risk profile, enrolment to a service can take place through existing identity and access management processes, for example, where a user access request occurs via a request from the user with approval from the line manager. In higher risk scenarios there could be a requirement for re-verifying the user's identity and potentially re-verifying the device for which enrolment has been requested. A third scenario would enable automation, where a user logs-in using existing credentials to enrol potentially supplemented with answers of relevant security questions (staff number, parts of address, age, start date in organisation etc.). Identity services will generally be independent of the type of end-point devices.

As is the case for mobile devices, the management of identity for laptops, thin clients and desktops are not handled at the device level. Each Government organisation should manage identities centrally. The question is how the user authenticates to prove that they are who they claim to be.

### 6.5.3.2 ACCESS CONTROL SERVICES

Access controls will apply at different levels. User authentication is the act of establishing a user is who they state they are. Often authentication occurs through logging in to on a website giving access to the business services. This can be supplemented by a second factor:

- Something a user knows – e.g. a password
- Something a user is – e.g. a fingerprint, an iris match or another biometric
- Something a user has – e.g. a technical factor such as a static IP, a device ID or alternatively a soft or hard token.

## Access Control at Device Level

Access control will happen at different levels. For example access to a smartphone will typically be through a pin and complex password.

The second step is to access government resources, such as business applications or the Intranet. Doing so will require a login using username and password. For higher impact applications/functionality this first factor can be supplemented with a second factor. A second factor could include:

- Device fingerprinting using http headers, browser versions, OS versions, languages and time-zone and
- Additional factors such as flash cookies, physical tokens or soft tokens.

Authentication could either happen against a specific second factor (such as a token) or as a risk based decision (using a combination of input such as factors, fingerprints, usage patterns). In a risk based authentication model a low risk score can trigger a second method of authentication such as:

- A one-time password using SMS or similar
- Challenge questions (something the user knows)

If the risk score is under a certain threshold, access could be denied altogether or even an escalation for incident investigation. The decision of authentication method could happen based on which resource the user is trying to access, e.g. access to the Intranet is allowed using username and password whereas access to business applications require a second factor or risk based decision.

The following model illustrates the types of controls an organisation should consider in a defence in depth model with mobile device end-points.

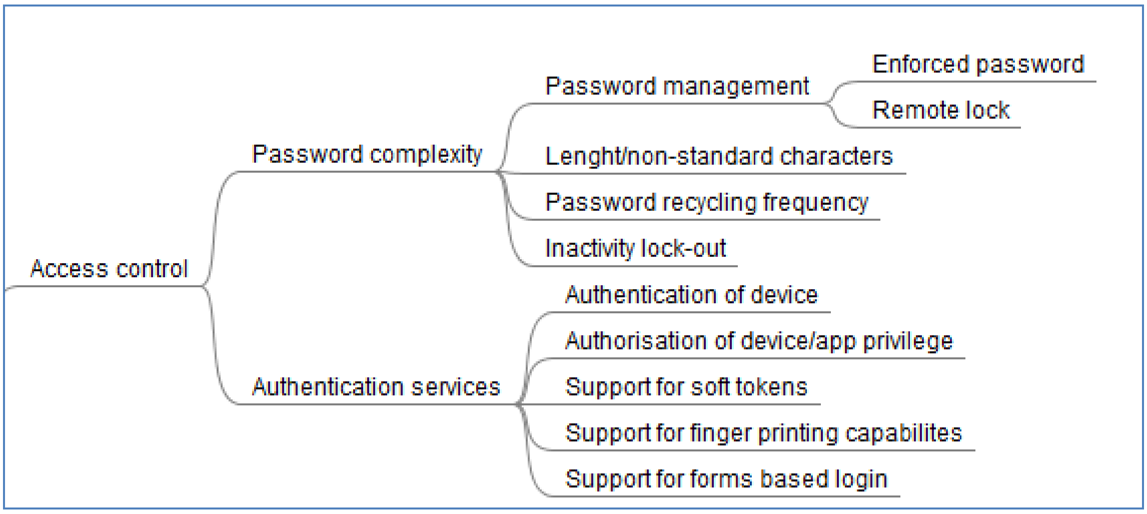


**FIGURE 6 - ACCESS CONTROL**

There are very few fundamental differences between smartphones, desktops, laptops and thin clients when it comes to authentication. Users can typically leverage the same authentication mechanisms across devices. Differences worth mentioning include:

1. The protection profile of each device – some mobile devices do not support strong encryption or strong authentication upon access which could lead to a risk decision not to allow that device type to access higher impact services or to require an additional factor for access to such services. A smartphone can be re-routed to an intelligent device and duped into providing false reports. This way, devices may report that they are encrypted, when actually they are not.
2. The physical location of the device – for desktops and thin clients you can physically secure the devices, meaning that there can be a decision to require less device based authentication as the physical premises already imposes a second factor of authentication (such as proximity passes to enter protected areas).

### 6.5.3.3 ENCRYPTION SERVICES

Due to their inherently mobile and valuable nature mobile devices are at increased risk of theft. The same applies to laptops, whereas generally PCs will be located in physically secured facilities where a decision not to encrypt the hard drive could be a sensible risk decision in the interest of cost.

The risk of loss of a device increases when mobile devices are used for sensitive information of various types that could be of interest for targeted attacks. The main risks to consider are confidentiality of the data on the device as well as the risk that a compromise is used as a means to gain access further into the core of the organisation, e.g. to business applications.

Encryption is the main defence against loss of confidentiality of information on the device. Some mobile devices can provide native encryption, but in other instances an organisation may have a requirement for using additional solutions. Requirements driving such an investment includes if there's a need to enforce the encryption or type of encryption, or alternatively if the native encryption mechanism is not trusted and a different (stronger) mechanism is needed.

In addition, and in line with the PSN Operational Security Architecture, confidentiality can be required to be enforced at the data level as opposed to device level. Different architectures could be used but the PSN architecture discussed PKI using certificates to encrypt and sign messages for messages containing sensitive information.

If it is deemed secure for a user to read such messages on mobile devices, this could be achieved by loading the user's certificates onto the device. Alternatively, where certificates are not loaded onto the mobile devices, the PKI encryption could be used to enable central users to send encrypted messages from their laptops/desktops and not risk these messages being compromised on theft of less secured mobile devices replicating emails.

The following model outlines some of the relevant features to look for in a Mobile Device Management (MDM) solution from a security point of view, both for encryption but also for other confidentiality measures such as remote wipe.

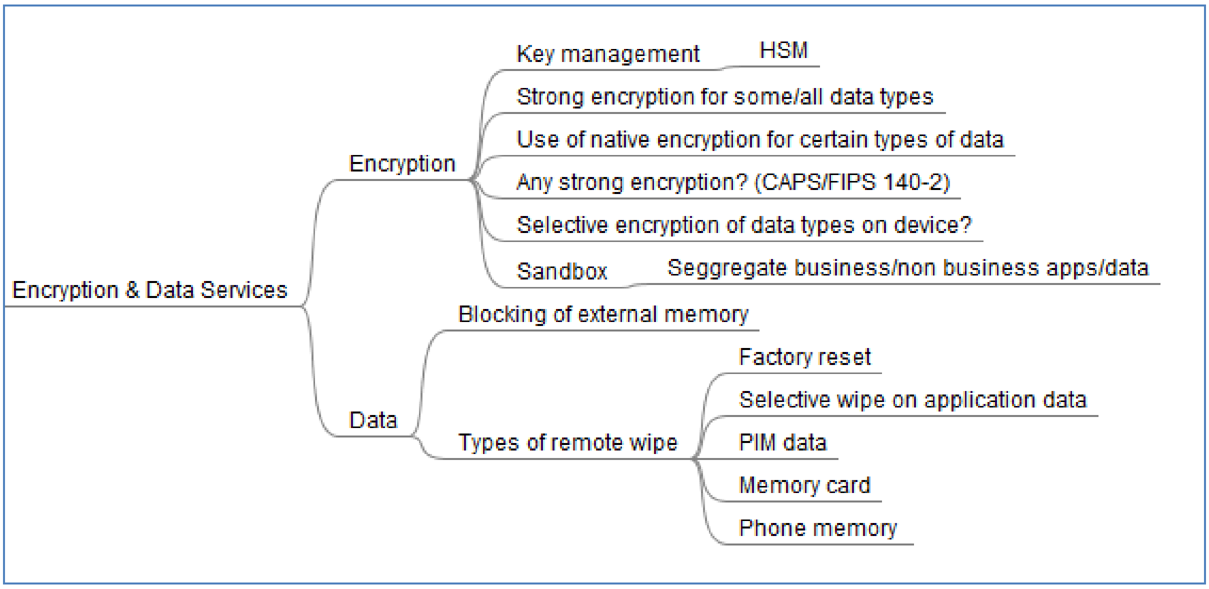

Encryption & Data Services
Encryption
Key management
HSM
Strong encryption for some/all data types
Use of native encryption for certain types of data
Any strong encryption? (CAPS/FIPS 140-2)
Selective encryption of data types on device?
Sandbox
Seggregate business/non business apps/data
Data
Blocking of external memory
Types of remote wipe
Factory reset
Selective wipe on application data
PIM data
Memory card
Phone memory

**FIGURE 7 - ENCRYPTION AND DATA SERVICES**

Both laptops and mobile devices are difficult to physically secure. Since devices such as these are more likely to be subject to theft, the attacker has more opportunity (time and resources available) to compromise any access controls or encryption. This means that typically such devices will be encrypted. The main difference between smart phones and laptops is the capabilities of the devices to enable encryption and the strength of the access control available. Due to greater maturity laptops would typically be secured with strong encryption.

The main difference between mobile devices and desktop devices, such as PCs and thin clients, is that the latter can be physically secured in the office environment which reduces the need for encryption as physical controls from the facilities can be leveraged. Another way of controlling the risk of compromise on the device is to lock down the ability to save data locally. The last major difference is that desktops and laptops have USB ports and these can be used to compromise the confidentiality of locally stored or centrally accessed data.

#### 6.5.3.4 Network Security Services

Devices connecting to the PSN must comply with the PSN IA requirements.

Relevant services would include:

- Firewalls and anti-virus software on each device
- Intrusion detection on the core network being accessed by the mobile devices
- Vulnerability management including scanning
- Penetration testing on critical infrastructure
- Patch and change management on all devices/services
- Hardening on all services

#### 6.5.3.5 Monitoring and auditing services

Through the layers of the security model it is important to enable monitoring and logging for security related events. This must be done using MDM technology on the devices, and should additionally be implemented at the network level and in the business applications to avoid malicious activities.

The relevant services and therefore events for monitoring and auditing will depend on the security policy and the risk profile of usage. At a high level, an organisation should consider at least the following:

- Logging capabilities for relevant events
- Vulnerability management
- Forensic analysis

The following model outlines some of the controls and events that an organisation should consider in their monitoring and auditing services on mobile devices. Operating system and application capabilities would typically be used to provide equivalent audits on PCs and laptops.

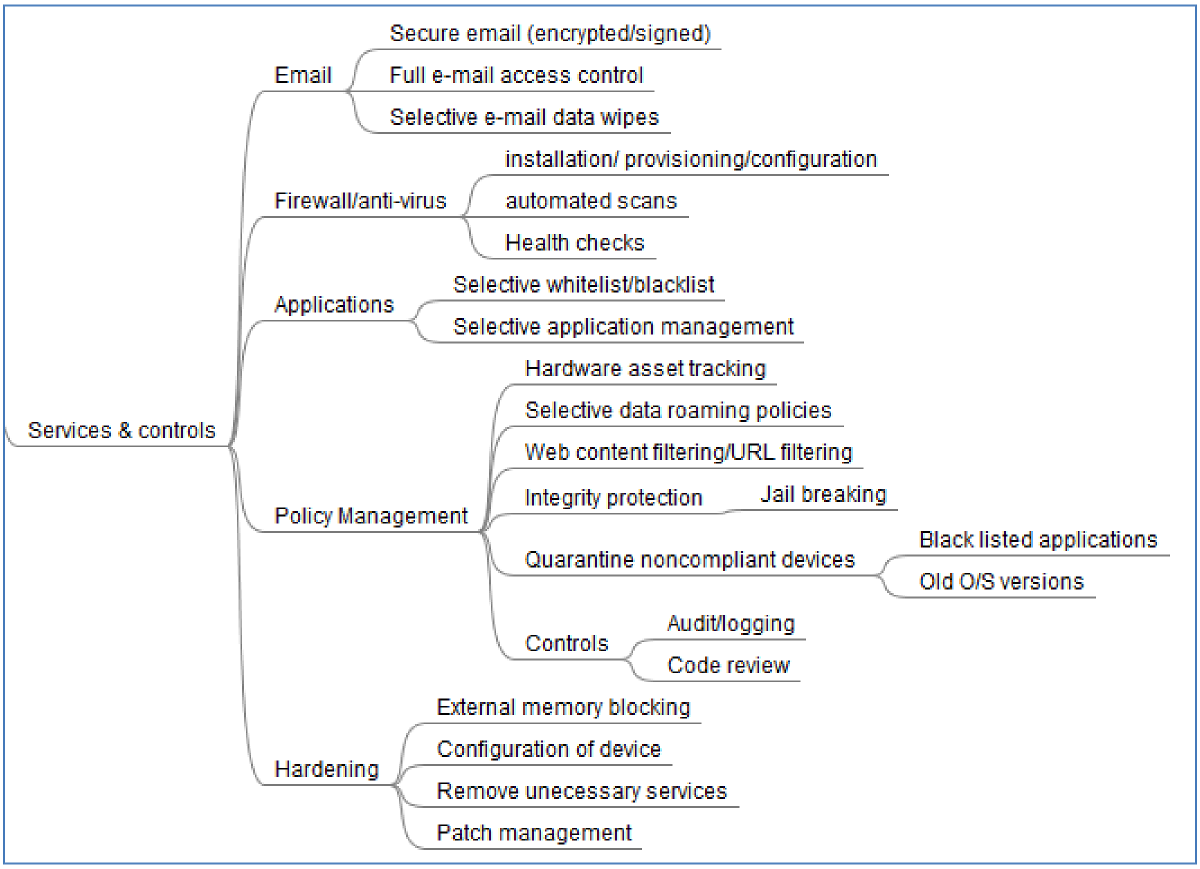

Services & controls
Email
Secure email (encrypted/signed)
Full e-mail access control
Selective e-mail data wipes
Firewall/anti-virus
installation/ provisioning/configuration
automated scans
Health checks
Applications
Selective whitelist/blacklist
Selective application management
Policy Management
Hardware asset tracking
Selective data roaming policies
Web content filtering/URL filtering
Integrity protection
Jail breaking
Quarantine noncompliant devices
Black listed applications
Old O/S versions
Controls
Audit/logging
Code review
Hardening
External memory blocking
Configuration of device
Remove unecessary services
Patch management

FIGURE 8 - SECURITY SERVICES AND CONTROLS

### 6.5.4 Security Technology

The following outlines the specific area of Mobile Device Management (MDM) and supplementary products for any gaps this technology offers from a security point of view. Similar technologies such as encryption, anti-virus and firewalls for desktops, thin clients and laptops are discussed throughout this Framework.

#### 6.5.4.1 Mobile Device Management

Mobile device management is a high growth area with a number of vendors positioning to meet the requirements of large enterprises needing to have assurance and control of the increasing use of mobile devices. The following summarises some of the main features in mobile technologies with specific focus on security.

| Mobile Security Solution | Pros (most solutions) | Cons (most solutions) |
|---|---|---|
| **Mobile Device Management** | • Centralised device and configuration management<br>• Policy Enforcement (i.e., device | • Interoperability across platforms<br>• Lacks malware detection |

| | | |
|---|---|---|
| | settings, password policy)<br>• Remote Wipe Capabilities<br>• Enhanced encryption<br>• Mobile Application Management and deployment | • Limited separation of corporate and personal data<br>• Lacks ability to detect unauthorised connects and outbound transmissions |

TABLE 37 - MOBILE SECURITY SOLUTIONS

Mobile Device Management (MDM) tools differ in their capabilities and focus. This is no different to most commercial off the shelf software (COTS) products and means that in order achieve acceptable risk levels devices need to be seen as part of a wider environment and a defence in depth approach is vital. This includes controls in backend systems, controls in the wider infrastructure and controls in the applications running on the devices. To provide a high level indication, some of MDM approaches have been summarised in the next table:

| **Mobile Security Solution** | **Pros (most solutions)** | **Cons (most solutions)** |
|---|---|---|
| **Mobile Anti-Virus** | • Mobile Malware Identification and Sanitization<br>• Spyware Detection and Removal<br>• Mobile Application White-listing | • Limited interoperability between device platforms for centralised management and compliance validation |
| **Mobile Application Code Review** | • Embedded vulnerability device in binary or source code | • Licensing – potential compromise of source code |
| **Secure Mobile Voice Encryption** | • Provides strong encryption for voice calls | • Interoperability between devices (hardware and software limitations) |

TABLE 38 - MOBILE SECURITY SOLUTIONS

Other factors should be taken into account when identifying and designing MDM solutions. These are not covered in detail in this document, but include:

- Delivery model (on premise, hosted, SaaS etc).
- Management capabilities (e.g. software distribution, policy management, inventory management, service management, self-service management, problem management).
- Reporting (both for security and other management capabilities).
- Integration capabilities (e.g. with Service management tools).

- Platform support, including for critical controls such as strong encryption (e.g. iOS, Symbian, Windows).
- Vendor considerations (e.g. financial strength).
- Software distribution (e.g. application downloader and update support)

## 6.6 Web Development Standards

When the world wide web was first established, most of the data being served by internet was in form of static content. A static page is stored on a web server and does not change over the period of time. Users requesting a specific resource were served by the web server with file/resource stored on their physical media.

As the web evolved, dynamic content became the primary mechanism of delivery. Dynamic content has the capability of delivering a set of data to a user based on user supplied criteria, user's credentials and other parameters. Today most of the internet traffic takes the form of dynamic content.

Static or dynamic, no matter what content type is being delivered, a page is structured using basic building blocks – scripting languages which define the page, and add-on layers which can extend page's look and feel, functionality etc. HTML (W3, 2012) is the page definition language through which pages are 'defined' and sent to a browser. To extend the looks of the page cascaded style sheets (CSS) are used. CSS helps maintain uniformity across a page's look and feel definition. To perform client side activities, such as validations and custom graphics painting etc, JavaScript is used prominently.

The core standard technologies for web applications are HTML for page content and markup, CSS for page design and styling, and Javascript for client side dynamic function.

The use of proprietary extensions such as Flash, Silverlight, or other ActiveX browser controls, beyond the core common web standard technologies should be avoided because they create potential dependencies on a single supplier or vendor, limiting flexibility to change or refine IT systems. They also create barriers to those users who do not, or cannot, use such extensions. The downstream cost implications of such apparently "free" extensions must be considered in full.

### 6.6.1 Legacy Web Application Compatibility

Changes in mark-up interpretation mean that some web applications may not function correctly in old versions of browsers. Additionally if web applications are not maintained for current browser technology standards, the users may experience problems with applications. To solve the issue of "old applications on new browsers" workarounds exist, for example, internet explorer plugins through products such as Browsium's Ion. To minimise this problem, web applications should conform to the core common standards which are unlikely to be implemented differently over time.

## 6.7 CESG Guidelines

CESG Information Assurance (IA) Good Practice Guides (GPGs) provide guidance on specific aspects of IA in order to help manage risk effectively.

- CESG Good Practice Guide No. 1 - Superseded with parts of IS4*. The original guide related to secure telecommunications
- CESG Good Practice Guide No. 2 - Advice On Handling Files With Possible Malicious (Content superseded with parts of IS4)
- CESG Good Practice Guide No. 3 - Securing Bulk Data Transfers *
- CESG Good Practice Guide No. 4 - Remote Access to PROTECT Data *
- CESG Good Practice Guide No. 5 - Securing Data At Rest On Laptops *
- CESG Good Practice Guide No. 6 - Off-shoring: Managing the Security Risks
- CESG Good Practice Guide No. 7 - Protection from Malicious Code
- CESG Good Practice Guide No. 8 - Protecting External Connections to the Internet
- CESG Good Practice Guide No. 9 - Taking Account of the Aggregation of Information
- CESG Good Practice Guide No. 10 - Remote Working *
- CESG Good Practice Guide No. 11 - KVM Switches
- CESG Good Practice Guide No. 12 - Use of Virtualisation Products for Data Separation: Managing the Security Risks
- CESG Good Practice Guide No. 13 - Protective Monitoring for HMG ICT Systems
- CESG Good Practice Guide No. 14 - UK Requirements for TEMPEST Countermeasures *
- CESG Good Practice Guide No. 15 - Auditing Compliance with HMG Information Assurance Standard No. 6
- CESG Good Practice Guide No. 16 - Taking Cryptographic Items overseas*
- CESG Good Practice Guide No. 17 - Client System Security
- CESG Good Practice Guide No. 18 - Forensic Readiness
- CESG Good Practice Guide No. 19 - Managing Accreditation - Governance, Structure & Culture
- CESG Good Practice Guide No. 20 - ICT Service Management - Security Considerations
- CESG Good Practice Guide No. 21 - Video Conferencing
- CESG Good Practice Guide No. 23 - Assessing the Threat of Technical Attack Against ICT Systems CESG Good Practice Guide No. 24 - Security Incident Management
- CESG Good Practice Guide No. 27 - Online Social Networking
- CESG Good Practice Guide No. 28 - Improving Information Assurance at the Enterprise Level
- CESG Good Practice Guide No. 29 - ICT Security Aspects of Collaborative Working
- CESG Good Practice Guide No. 35 - Protecting an Internal ICT Network

* denotes controlled material.

Extracts taken from HMG Documentation. © Parts of this document are copyright, reserved and vested in the Crown. For more information from CESG, please visit: www.cesg.gov.uk

## 6.8 Bring Your Own Device

### 6.8.1 Benefits of BYOD

BYOD programmes can offer real benefits to employees. While the table above details BYOD from a device perspective, it is essential to recognise that the consumerisation of IT is not just about the Technology. Although technology is the enabler, at its core BYOD is about how people work and encompasses policies, processes and technology.

BYOD can deliver the following benefits:

- Allows users to work in ways they want to on devices they want to. Users work in different ways and BYOD can free users to work smarter and be more productive.
- Provides the opportunity to use smartphones and tablets in 'dead time' (e.g. during travel).
- Devices can meet user demands enabling them at work, rather than acting as an inhibitor
- Delivers continuity to businesses as employees can work from alternate locations when they can't get to the office.
- Allows organisations to embrace the already growing trend of BYOD in a corporately accepted and controlled way.
- Retains talent without additional costs as consumer technology is a strong factor in career selection for younger employees.
- Offers users the ability to bring their 'best of breed' consumer technology to work.

### 6.8.2 Considerations For BYOD

Before implementing BYOD in an organisation, it is important to start with a Vision or Strategy identifying the keys aims and benefits at the outset. Each organisation is unique, with its own challenges; identifying the outcomes and behaviours to drive will enable the solution to create value and be realistic.

Organisations should pay particular attention to the TCO, and also to any legal and tax issues associated with BYOD. This can be particularly important if the organisation is subject to particular legislative and regulatory controls. Policies and procedures should be comprehensively reviewed before introducing BYOD, to ensure that both the organisation and user have clear and defined responsibilities and liabilities.

Successful deployment of BYOD depends on a device meeting a minimum level of functionality, agreed by the organisation, and aligning a number of factors. Security concerns are likely to be a key issue for an organisation – these are considered in depth in Section 6.5. The following sections will outline and provide details on some of these.

**Buy Your Own or Bring Your Own**

Consumerisation can include both *bring* and *buy* your own device elements, including a mixture of the two. The table below summarises the key differences between these approaches.

| Buy Your Own | Buy Your Own & Bring Your Own | Bring Your Own |
|---|---|---|

| | | |
|---|---|---|
| Driven by user's desire to use non-standard devices with an expectation to receive some financial recompense.<br>Would be expected to replace a corporate device and have some financial benefits to the company.<br>For example, allowing users to buy MacBook's rather than receive the organisation's laptop. | It is possible to allow for both scenarios to avoid alienating users who want to work more efficiently on different devices.<br>Bring Your Own Device users are allowed to access certain data or applications in controlled ways.<br>Buy Your Own Device users are financially rewarded because their take-up of BYO results in lower costs. | Driven by user's demand to use their own devices for work purposes with no financial incentive.<br>May replace corporate mobile device but unlikely to replace main corporate device. Personal device is a supplement not a replacement.<br>For example, using a personal iPad to receive company mail when out of the office but still using a corporate machine for most job functions. |

**TABLE 39 – COMPARISION OF BYOD MODELS**

**Policies and Procedures**

Organisational policies need to be reviewed and, if necessary, updated to reflect 'good use' of personal devices. For example, policies should state the need for employees to purchase insurance and warranty for device so that they can be replaced or repaired. Organisations should also consider whether they will require more insurance to protect against damage to employee kit.

Procedures will also need to be established for the approval, financial (stipend) and security access processes. Organisations should also consider any impact on their Human Resources and Health and Safety policies relating to the use of BOYD, especially whilst at home etc.

Successful BYOD schemes are dependent on a strong framework to guide users through the scheme. The following table details some key governing rules that should be considered as the foundations for high user uptake. These rules are not exhaustive and if an organisation is considering introducing BYOD, the organisation should undertake a comprehensive readiness assessment and ensure policies and procedures are updated sufficiently before the scheme is introduced.

| **Rule** | **Buy Your Own** | **Bring Your Own** |
|---|---|---|
| User and device registration is mandatory and for a set period | ✓ | |
| Participation is subject to line manager approval | ✓ | ✓ |
| Financial stipend is fixed and must cover the enrolment period | ✓ | |
| Users will not receive any additional stipend / corporate device during scheme enrolment | ✓ | |

| | | |
|---|---|---|
| Users should have relevant warranty and insurance | ✓ | |
| Once scheme is established new enrolments should coincide with laptop refresh cycles | ✓ | |
| Computer based training must be completed and audited, including annual policy requirements like security and compliance | ✓ | ✓ |
| Participants to agree with amended policies including HR, Health and Safety and Legal | ✓ | ✓ |
| Participants to agree to pay back (pro rata) the stipend if they leave the company within the enrolment period | ✓ | |

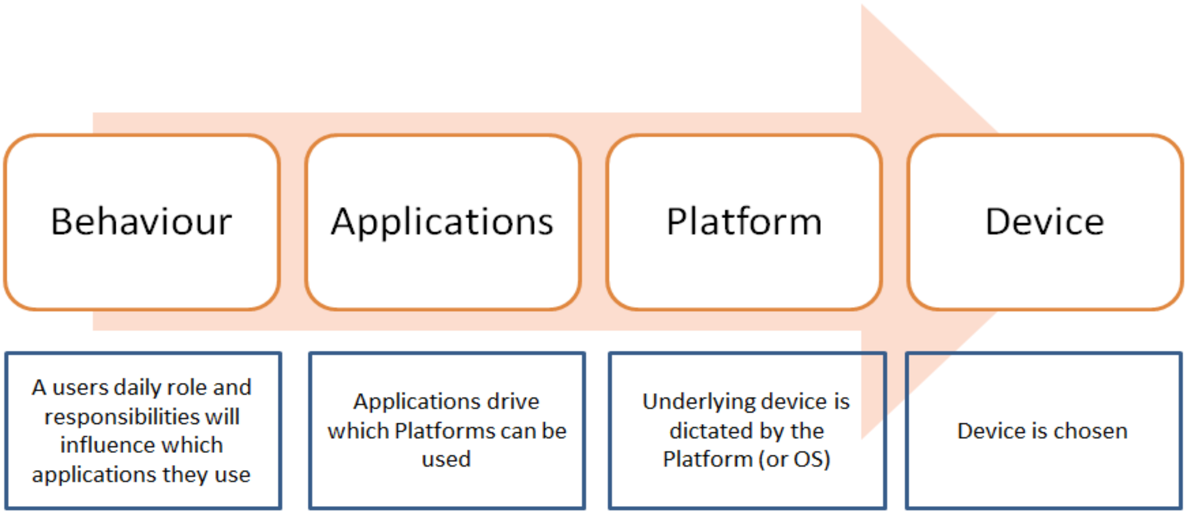
**TABLE 40 – EXAMPLE POLICIES AND PROCEDURES**

**Devices**

A BYOD model requires organisations to decide whether to let users bring any device, or whether to impose restrictions. Restrictions may stem from security concerns, for example, Android smartphones are very popular consumer devices, but are difficult to secure. For more information on device security refer to section 6.5 of this document.

If organisations want to define which devices employees can use, then they need to select the appropriate devices depending on what activities users need to perform. Employees work in different ways and perform different roles, and it is important that their device supports users in their job functions. One way to determine which devices should be recommended to particular employees is user segmentation (section 7 in part 3 of this document).

The following figure illustrates how the behaviour of users and the applications they need drives the platform and devices they require:


Behaviour
Applications
Platform
Device
A users daily role and responsibilities will influence which applications they use
Applications drive which Platforms can be used
Underlying device is dictated by the Platform (or OS)
Device is chosen

F

**IGURE 9 – BEHAVIOUR DRIVES BYOD DEVICE CHOICE**

It should be noted that not all devices are suitable for all users. For example, an employee who needs to carry out data input will not be able to work efficiently from a smartphone, even if the appropriate application could run on the device.

The consumerisation of IT is about how people work, as well as which device is selected. For example, producers of content may favour devices that provide a rich user experience, whereas travellers and consumers of content may select highly portable and easy to hold devices with limited functionality.

**Eligibility and Adoption**

For a successful BYOD programme, organisations must consider who in their organisation should be eligible to participate. It is often assumed that BYOD schemes are more successful and inclusive where offered to as many employees as possible. However, there are roles, such as Call Centres operatives (Line of Business users), where consumerisation would be an unsuitable option. On the other hand, a BYOD solution may be suitable to enable some Knowledge Users to be more productive when they are occasionally mobile.

Furthermore, organisations should recognise that BYOD is not a model that all employees will want to adopt. There are generational differences separating how people embrace technology, with younger employees potentially more likely to participate in at BYOD programme than those who are older.

To encourage adoption and user uptake an organisation should engage at all levels, clearly outlining the benefits to employees and aiding users to gain a good experience from their devices. Any BYOD roll out should have a through communications and change plan, detailing how user groups will be engaged and when.