SITA

Deployment Guidelines:
Personal Computing Devices

Version:	2.1
Date:	2024-03-25

Notice

Document enquiries may be directed to:
Records Management Office
SITA SOC Ltd
PO Box 26100, Monument Park, 0105, South Africa
Tel: +27 12 482 3000
www.sita.co.za

Deployment Guidelines: Personal Computing Devices
Document No: **eNSQS-00146**
Version: **2.1**
Author: **Izak de Villiers**, izak.devilliers@sita.co.za, +27 12 482 2749

Approval

The signatories hereof, being duly authorised thereto, by their signatures, hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

27 March 2024

Tshavhu Mukhodobwane
HOD: Norms Standards and Quality

Date

GA Nel

25/03/2024

Deon Nel
Senior Specialist: TAS

Date

IdeVilliers

25 March 2024

Izak de Villiers
Senior Specialist: TAS

Date

Foreword

This document forms part of best practices guideline and solution selection process for Personal Computing Devices, enabling cost-effective procurement and deployment of ICT by Government. The goal is to enable Government to procure and deploy appropriate technology solutions for its business requirements. The Deployment Guide is intended to inform the ICT architecture of Government departments in terms of usage models, hardware and infrastructure requirements. It supports any procurement vehicle for PCDs, including Transversal Contract 740 or *ad hoc* processes. **Complete, turnkey** solutions are in view, including all required components and associated services (e.g., supply, installation, training, support and maintenance).

Contents

Tables

Figures

1. Introduction and background

This document recommends deployment practices for the **Personal Computing Devices** technology domain (including client computing devices, desktop displays and mobile devices), and provides guidelines, standards and advice for the appropriate selection and deployment of the available technologies. The main purpose of the Deployment Guide is to inform end users about best practices and cost-effective, optimal utilisation of available solutions.

Technology Advisory Services (TAS) created these guidelines as part of SITA's mandate to enable efficient and cost-effective use of ICT in Government. The guidelines are an output of the unit's standard research, specification and consultation processes, drafted in collaboration with clients (including GITOC bodies), suppliers and manufacturers.

The document contains both **normative** and **informative** guidelines. Informative guidelines point out best practices and other helpful information, while normative guidelines are **mandatory** for Departments, and deviations may result in audit findings.

The guidelines are not intended to replace Departmental ICT policies and processes, but should complement these while focussing on adding value during the entire ICT lifecycle. Applicable guidelines should be used in conjunction with other related documentation, including any relevant Contract Engagement Models, contract conditions, definitions and technical specifications.

Many specialised or niche requirements are not addressed in the document, and should be handled on a case-by-case basis, with input from TAS where required. A sample RFQ is included in **Annex A**, to be used when publishing requests for quotation/proposal.

Experience with Government requirements and requests for quotation has shown that many Departments copy technical specifications from industry sources, instead of writing their own. Since this compromises fairness and an adequate definition of the actual business requirement, the Deployment Guide promotes open, unbiased specifications and focusses on end-user needs.

1.1 References

The following documents are referred to in this document, or have an impact on the implementation of the processes described herein:

- Legal framework:
  - The Constitution of RSA, Act 108 of 1996
  - Public Finance Management Act (Act 1 of 1999, as amended)
  - State Information Technology Agency Act (Act 88 of 1998, as amended)
  - SITA Regulations, 23 September 2005
  - National Treasury Practice Note no. 5 of 2009
- Contracts:
  - Master Agreement: Personal Computing Devices and Peripherals (Transversal Contract 740)
  - Engagement Model: Personal Computing Devices and Peripherals (Transversal Contract 740)
- Processes and documents:
  - Technology Certification Process (eNSQS-00144), version 4.0, March 2022
  - SITA Product Certification: OEM Memorandum of Agreement (eNSQS-00145), version 2.2, May 2023

- SITA Product Certification website www.sita.co.za/prodcert.htm:
    - Latest versions of technical specifications for all technology domains
    - All related information, documents and forms
- Related research:
    - TAS Research Report: Desktop Windows Security and Optimisation, version 2.0, June 2023
    - TAS Research Report: Procuring ICT Products from Retail Stores vs. Transversal Contracts, version 3.0, June 2020

1.2 Standardisation

Standardisation helps Government to realise the ICT House of Value (as defined in the Government Wide Enterprise Architecture), which includes economies of scale, interoperability, reduced duplication, digital inclusion, universal design and security. Standards can be defined and implemented at various levels, including the following:

- Open industry standards (*de jure*): These include standards such as those published by the IEEE, IETF and ISO/IEC, e.g. TCP/IP, USB, PCI, HTML, ODF, ISO/IEC 60950, RFC 3261. These standards are required for basic interoperability in the ICT environment. Interoperability standards in Government are stipulated in the Minimum Interoperability Standard (MIOS), as well as other formally-accepted specifications, either per Department or Government-wide.

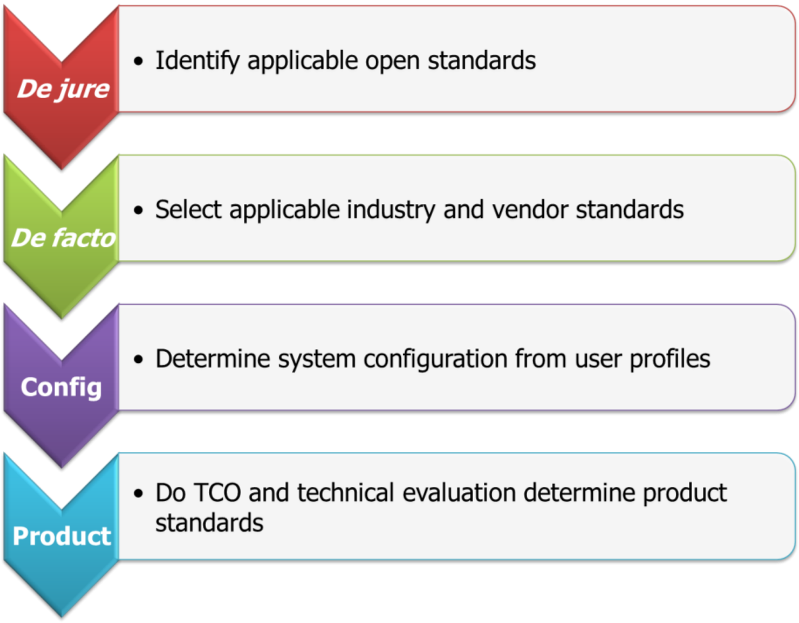

De jure
• Identify applicable open standards
De facto
• Select applicable industry and vendor standards
Config
• Determine system configuration from user profiles
Product
• Do TCO and technical evaluation determine product standards

Figure 1: Standards selection process

- **Generally-accepted vendor and industry standards (*de facto*):** These are not open standards, but they are so widespread that the industry needs to conform to them to meet interoperability requirements. Environments and applications such as Microsoft's Windows and Office products may be included here. Like open standards, these standards also enable interoperability, but more by virtue of their wide deployment (e.g. Windows is estimated at >90% penetration in the desktop computing sphere) than inherent superiority. Another example of this is Android in the mobile space.
- **Configuration standards:** This is where an organisation defines a specific configuration of device per user functional profile. Configurations should primarily be informed by business needs. This standard can be used as a procurement and communication tool within the organisation. For example, a single master system image can be used to ensure all devices are configured the same way.
- **Product standards:** Configuration standards can apply to selecting a standard brand and model that conforms to the stated configuration requirements. This can ease the burden associated with ICT operational issues such as procurement, support, logistics and maintenance. For example, maintaining several different product standards is more expensive in terms of user productivity and IT effort to manage multiple software configurations. Departments are encouraged to standardise down to product level to reduce complexity and improve interoperability within the Department.

This document recommends a process whereby Departments can move from *de* jure standards through *de facto* and configuration to arrive at product standards that meet business requirements.

1.3 Design principles

Based on Government's technology and business goals for ICT procurement, the following principles were incorporated into the design of all technology domains:

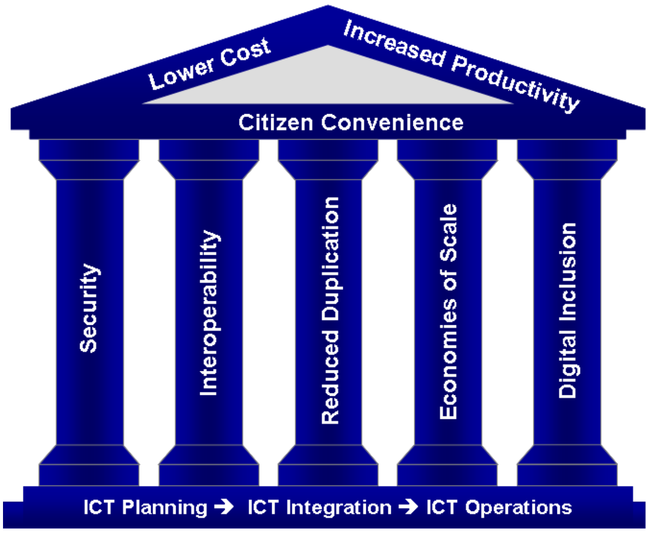


Figure 2: ICT House of Value

- Support for the ICT House of value:
  - Security
  - Interoperability
  - Reduced duplication
  - Economies of scale
  - Digital inclusion
  - Lower cost
  - Increased productivity
  - Citizen convenience
- Best-fit solutions for client requirements via usage profiles.
- Industry standards.
- Scalability and upgradeability.
- Enterprise-class functionality and design, including security and manageability.
- Integrated service offering: standard on-site SLA included in all solutions.
- Environmental sustainability.
- Support for all mainstream operating environments for end-user computing.
- Specification is product- and brand-agnostic, focussing purely on industry standards and functionality.
- "Equal or better" principle: products with functionality equivalent to or exceeding specifications are acceptable.
- Lowest possible technology baseline based on requirements: solutions that exceed specifications require Government to spend money on unnecessary functionality and capacity.
- Standards and specifications approved by appointed Government bodies, e.g. GITOC structures such as SC-ITSM.
- Local economic development:
  - Support for regional procurement, service and support to build skills and capacity in the local ICT industry by mandating OEMs to train and certify SMME/BEE suppliers.
  - Ensure sustainability for suppliers, including small regional players: empower BEE/SMME organisations to build a sustainable business supplying and servicing Government infrastructure.
  - Support local industry (e.g. manufacturing) where appropriate.

1.4 Processes

1.4.1 Product certification

According to the SITA Act, the Agency must certify ICT goods and services to ensure that they conform to Government ICT standards, policies and service requirements.

To support this mandate, SITA has developed, in collaboration with DCDT, GITOC, Government stakeholders and industry, a **Technology Certification Process** (TCP) according to which specific classes of products can be certified. At the time of writing, these classes of products include the following technology domains, with the domain under discussion emphasised.

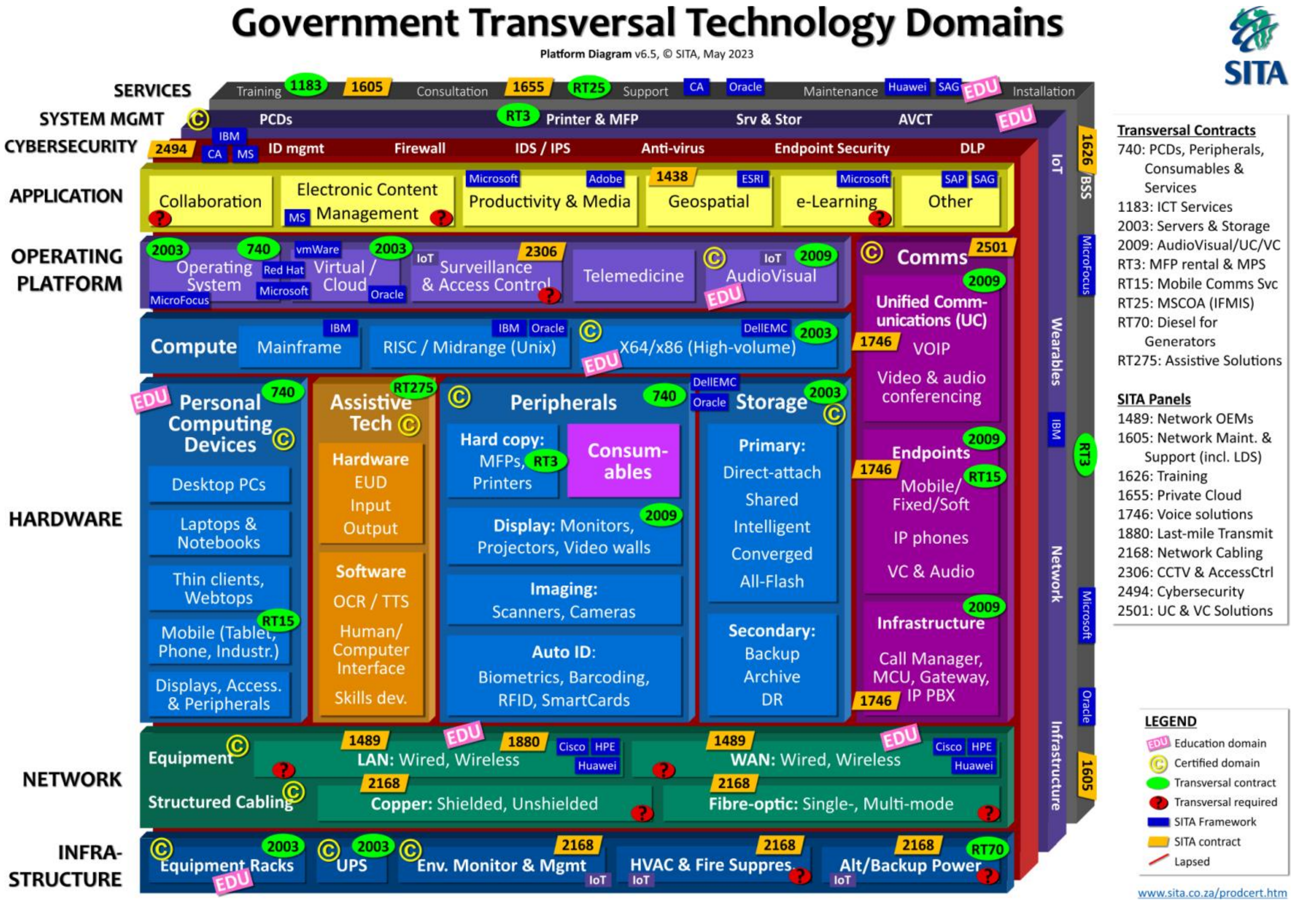
Domain	Components
Personal Computing Devices	**Desktop PCs, Mobile PCs, Desktop displays, Mobile devices (Tablets, Smartphones, Industrial handhelds), Accessories and Device Management**
Peripherals	Printers, Multifunction devices, Scanners, Digital cameras, Automatic Data Capture (Barcoding, Card devices), Biometric readers, Consumables and Print management
Assistive Technologies	Assistive devices and software for people with disabilities, including smart devices (tablets, PDAs, readers, media players, recorders and braille devices), peripherals (input and output devices) , assistive software enabling access and speech (AAC), and skills development and learning aids for users with disabilities
Education Solutions	Classroom solutions, including PCs, laptops, tablets, presentation and teaching devices, Classroom infrastructure and systems (hardware and software), and e-Sports systems
Audiovisual Communications (AVC) Technologies	Video and audio conferencing, large-format display devices (projectors, monitors, interactive displays and display walls), collaboration, media recording, speech processing, and AV signal control and management
Surveillance & Access Control (SAC)	Fixed and mobile surveillance and physical access control solutions, including IP cameras, mobile cameras, UAVs, storage and recording devices, video management systems and control room solutions
Servers & Storage	Servers (Rack-mount, Tower, Blade), Primary storage and Secondary storage (Disk to disk, Tape automation and Archiving)
Networking	LAN, WLAN and WAN equipment, Wireless backhaul, and Structured cabling (copper and fibre-optic)
Infrastructure	UPS, Equipment Racks, Alternative power, Cable ducting, trenching and routing
Cybersecurity	Cybersecurity products and solutions (ISS – information system security)

Table 1: Technology domains within the TCP

The Technology Certification Process requires OEMs to register with SITA, and thereafter submit their products for certification according to the standard product evaluation process. Products are measured against approved specifications and, if compliant, certified and listed in a Certified Products Database. OEMs are encouraged to get their products certified at their earliest convenience.

Government often requires integrated solutions spanning multiple areas and technology domains. For example, PCs may be required as part of an AVCT solution for a Department. These PCs must be certified according to the requirements of the PCDs domain, even though the entire solution is procured via the AVCT domain. Equipment from the different domains must be integrated and supported by an OEM-approved service provider or supplier.

The Diagram below illustrates relationships between certified technology domains and indicates procurement contracts that have been established by SITA for Government use.



Government Transversal Technology Domains
Platform Diagram v6.5, © SITA, May 2023
SITA
SERVICES
SYSTEM MGMT
CYBERSECURITY
APPLICATION
OPERATING PLATFORM
HARDWARE
NETWORK
INFRA-STRUCTURE
Training 1183 1605 Consultation 1655 RT25 Support CA Oracle Maintenance Huawei SAG EDU Installation
PCDs RT3 Printer & MFP Srv & Stor AVCT EDU
2494 IBM CA MS ID mgmt Firewall IDS / IPS Anti-virus Endpoint Security DLP
Collaboration
Electronic Content MS Management
Microsoft Adobe Productivity & Media
1438 ESRI Geospatial
Microsoft e-Learning
SAP SAG Other
2003 740 Operating System MicroFocus Red Hat Microsoft
vmWare 2003 Virtual / Cloud Oracle
IoT 2306 Surveillance & Access Control
Telemedicine
IoT 2009 AudioVisual EDU
Comms 2501
2009 Unified Communications (UC)
1746 VOIP
Video & audio conferencing
Compute
IBM Mainframe
IBM Oracle RISC / Midrange (Unix)
DellEMC 2003 X64/x86 (High-volume) EDU
EDU Personal Computing Devices 740
Desktop PCs
Laptops & Notebooks
Thin clients, Webtops
Mobile (Tablet, Phone, Industr.) RT15
Displays, Access. & Peripherals
Assistive Tech RT275
Hardware EUD Input Output
Software OCR / TTS Human/ Computer Interface Skills dev.
Peripherals 740
Hard copy: MFPs, RT3 Printers
Consum-ables
Display: Monitors, Projectors, Video walls 2009
Imaging: Scanners, Cameras
Auto ID: Biometrics, Barcoding, RFID, SmartCards
DellEMC Oracle Storage 2003
Primary: Direct-attach Shared Intelligent Converged All-Flash
Secondary: Backup Archive DR
2009 Endpoints
1746 Mobile/ Fixed/Soft RT15
IP phones
VC & Audio
2009 Infrastructure
Call Manager, MCU, Gateway, 1746 IP PBX
Equipment
Structured Cabling
1489 EDU 1880 LAN: Wired, Wireless Cisco HPE Huawei
2168 Copper: Shielded, Unshielded
1489 EDU WAN: Wired, Wireless Cisco HPE Huawei
2168 Fibre-optic: Single-, Multi-mode
2003 Equipment Racks EDU
2003 UPS
2168 Env. Monitor & Mgmt IoT
2168 HVAC & Fire Suppres IoT
2168 RT70 Alt/Backup Power IoT
IoT
Wearables
Network
Infrastructure
1626 BSS
MicroFocus
IBM
RT3
Microsoft
Oracle
1605
Transversal Contracts
740: PCDs, Peripherals, Consumables & Services
1183: ICT Services
2003: Servers & Storage
2009: AudioVisual/UC/VC
RT3: MFP rental & MPS
RT15: Mobile Comms Svc
RT25: MSCOA (IFMIS)
RT70: Diesel for Generators
RT275: Assistive Solutions
SITA Panels
1489: Network OEMs
1605: Network Maint. & Support (incl. LDS)
1626: Training
1655: Private Cloud
1746: Voice solutions
1880: Last-mile Transmit
2168: Network Cabling
2306: CCTV & AccessCtrl
2494: Cybersecurity
2501: UC & VC Solutions
LEGEND
EDU Education domain
© Certified domain
Transversal contract
? Transversal required
SITA Framework
SITA contract
Lapsed
www.sita.co.za/prodcert.htm

Figure 3: Certified technology domains and transversal/period contracts

The latest version of the diagram is available at www.sita.co.za/prodcert.htm.

1.4.2 Technology evaluation and management processes

Technology domains are developed, evaluated and managed via a specific process and philosophy. The Constitutional requirements of fairness, equitability, transparency, competitiveness and cost-effectiveness are incorporated into all levels of the process. Government’s MIOS and MISS standards also inform the domain specifications. Domains are updated regularly via a collaborative process, with input from research, industry players, OEMs, Government bodies (GITOC) and end-users.

Technology evaluation process

Technical evaluation of products submitted for certification comprises both theoretical and physical evaluation via the following processes:

1) **Theoretical evaluation:** Technical verification of mandatory functionality, done in conjunction with the OEM during a product certification meeting. Only products that comply with all mandatory requirements are certified.

2) **Cost calculation:** Calculation of TCO based on OEM-supplied cost information.

3) **Physical test phase:** Laboratory tests and/or demonstrations of evaluation units (depending on domain and category).

    a) Validate supplied information via system tests and verification.

    b) Verify interoperability via compatibility tests.

    c) Measure performance using industry-standard benchmarks as well as methodologies developed in-house.

4) **Documentation:** Issue a formal product certificate to the OEM, capture certification details in a database of certified products, and store all submitted product information and test results.

Technology management process

Technology management is done on a continuous basis, and includes continually updating technology specifications (typically on a six-monthly or annual basis), certifying new products offered to Government, and replacing existing products with updated models.

Updates to specifications, minimum configurations, industry standards, etc. are managed via a formal Tech Update process. Tech Updates are published to the user community and industry, including OEMs and PCD suppliers for input before implementation. All changes to the technology specification are moderated and managed as an input to any procurement or tender exercise, which ensures that Government has a fair basis for comparing pricing and costs.

Model changes and the certification of new products are initiated by the OEM via a formal certification request, after which the new product is evaluated and certified via the standard Tech Lab process. Once the new product has been certified, the previous product may no longer be supplied to Government.

The technology management process is described in the document **Technology Certification Process** (see **References**). This process is mandatory for all technology domains within the TCP scope.

Certification process documents, forms and domain detail specifications are available at www.sita.co.za/prodcert.htm.

2. Overview of Personal Computing Devices domain

The purpose of the PCD technology domain is to specify and certify suitable products for deployment within Government, in support of any procurement vehicle utilised in this space (e.g. Contract 740).

2.1 Scope

The PCD technology domain comprises the following categories and technology types:

Category	Technologies
Desktop PCs	Standard PCs, all-in-ones, thin clients and workstations
Mobile PCs	Standard notebooks/laptops, tablets, workstations and ruggedised units
Desktop displays	Standard and advanced desktop displays
Mobile devices	Mobile phones, tablets and portable data terminals
Device Management	Device management tools and software

Accessories	Value-added peripherals and accessories for PCD systems

Table 2: Categories in the Personal Computing Devices domain

Detail specifications for all these devices are available at www.sita.co.za/prodcert.htm.

2.2 Domain goals and criteria

The following overall goals and evaluation criteria are integrated into the design of the PCD technical specification. Inputs from component manufacturers (e.g. for CPUs and storage), OEMs, industry research institutions (e.g. BMI-T, Gartner, IDC), and the client base (including GITOC TTT) form an important part of the process.

- Lowest Total Cost of Ownership. Supply chain regulations require Departments to measure TCO as part of the procurement process. TCO is dependent on the client and business requirement, and therefore an RFP/RFQ process must be used to define client needs on an *ad hoc* or project basis. To ensure the best possible TCO, the following elements are specified and/or measured during evaluation:
  - Usage profiles based on business requirements.
  - Reliability, availability and serviceability (RAS) of all solutions, including MTBF and MTTR ratings.
  - Comprehensive countrywide on-site SLA with upliftment options.
  - Manageability: Remote management, automated failure alerts, remote diagnostics and updates.
  - Duty cycles, work volumes and usage profiles.
  - Environmental factors such as power consumption and cooling requirements.
  - Other elements impacting productivity, including quality and usability.
- Service levels:
  - Comprehensive 3-year on-site warranty and 8-hour SLA.
  - Supplier training and certification by OEM.
  - Enabling of supplier service and quality levels via OEM process.
  - Dispute resolution between Government and industry.
- Performance and functionality: by taking into account low-level technology architectures, the best possible solution can be ensured for Government applications.
  - System architecture and functionality (e.g. 64-bit with virtualisation support).
  - Connectivity capabilities and options (e.g. WLAN and Bluetooth).
  - Processing capabilities (e.g. processor speed and memory capacity).
  - Upgrade options and accessories (e.g. storage, connectivity, docking solutions).
  - Security capabilities (e.g. physical locks, encryption, secure management).
  - Compatibility and interoperability (both hardware and software) via ISV and OEM certifications (e.g. Windows HCL, AutoCAD).
  - OEM-level certification according to specific standards (e.g. ISO/IEC quality and environmental standards).
  - Product-level certification according to SABS-endorsed electrical safety and radiation standards.
- Fair (“apples to apples”) comparison baseline for solutions, measured against an open, product-agnostic specification.

2.3 Domain components and usage profiles

The components of the PCD domain and related usage profiles as per the latest version of the detail specifications are listed below.

The usage profiles serve as an initial guideline to determine what type of system is required for a specific use case or type of user. The primary determining factor in selecting any ICT system is the **business requirement**, i.e. how the system will be used. To keep costs as low as possible, the basic principle is to select the smallest available system that supports the required functionality.

2.3.1 Desktop PCs

Item	Description	Usage profile
ThinClient	Thin / Zero Client	Thin or zero client device for server-based computing, supporting VDI, remote desktop or other host-based protocols
PC1	ChromeBox / Nettop PC	Low-cost desktop client device for entry-level use and Education; browser-based or low-end workflow
PC2	Entry-level PC (local)	Locally-manufactured entry-level office PC for basic office use; single-tasking, low-volume data requirement, task-oriented
PC3	Midrange PC	Midrange PC for higher-end applications (e.g. EIS, ECM, development); power users/knowledge workers with higher data/volume requirements, larger applications, multitasking
PC4	Advanced PC	Powerful PC for multitasking advanced applications with higher data and throughput requirements (e.g. media authoring, GIS, DTP, CAD, software development)
PC_AIO1	Entry-level all-in-one PC	Integrated (all-in-one) office PC with combined display and system unit for basic office use; single-tasking, low-volume data requirement, task-oriented
PC_AIO2	Midrange all-in-one PC	Integrated (all-in-one) business PC with combined display and system unit for higher-end applications (e.g. EIS, ECM, development); power users/knowledge workers with higher data/volume requirements, larger applications, multitasking
PC_WS1	Basic technical workstation, single-socket	Basic technical/engineering workstation for applications such as CAD, GIS, and DTP; technical workers with high data volumes and processing requirements. OpenGL- and ISV-certified. Single-socket CPU architecture
PC_WS2	Advanced technical workstation	Advanced technical/engineering workstation for applications such as CAD, GIS and DTP; high-end technical workers with extreme data volumes and processing requirements. OpenGL- and ISV-certified. Dual-socket CPU architecture

Table 3: Desktop PC usage profiles

2.3.2 Mobile PCs

Item	Description	Usage profile
Note1	Chromebook / Mobile thin client / Netbook	Low-cost laptop for entry-level use and Education; browser-based or low-end workflow
Note2	Value laptop	Basic/value laptop for cost-conscious users, offering mobility at the lowest practical price

Item	Description	Usage profile
Note3	Thin and light laptop	Thin and light/ultraportable laptop supporting extensive travelling; combination of highest mobility with mainstream functionality and performance
Note4	Midrange business laptop	Professional laptop with good balance between mobility and performance
Note5	Advanced business laptop	Advanced laptop with high performance and less emphasis on mobility
Note_Tab1	Convertible / 2-in-1 laptop	Highly portable touch- or pen-based laptop with 2-in-1, convertible or detachable design for touch or pen-based use
Note_WS1	Mobile technical workstation	Technical/engineering mobile workstation for CAD, GIS, DTP, etc; high-end technical workers with high data volumes and processing requirements. OpenGL- and ISV-certified
Note_Rugged1	Semi-rugged laptop	Semi-rugged laptop able to withstand regular operation outside office environments
Note_Rugged2	Fully rugged laptop	Fully ruggedised laptop for harsh environments, including extended operations in extremes of rough handling, dust, moisture and temperature (e.g. military and police operations)

Table 4: Mobile PC usage profiles

2.3.3 Desktop displays

Item	Description	Usage profile
Mon_DT1	Basic desktop display, 18"	Entry-level desktop display, 18"+ diagonal size
Mon_DT2	Basic desktop display, 21"	Entry-level desktop display, 21"+ diagonal size
Mon_DT3	Midrange desktop display, 24"	Midrange desktop display, 24"+ diagonal size
Mon_DT4	Midrange desktop display, 27"	Midrange desktop display, 27"+ diagonal size
Mon_DT5	Midrange desktop display, 30"	Midrange desktop display, 30"+ diagonal size
Mon_DT_Adv1	Advanced desktop display, 24"	Advanced desktop display with advanced features and ergonomics, 24"+ diagonal size
Mon_DT_Adv2	Advanced desktop display, 27"	Advanced desktop display with advanced features and ergonomics, 27"+ diagonal size
Mon_DT_Adv3	Advanced desktop display, 30"	Advanced desktop display with advanced features and ergonomics, 30"+ diagonal size

Table 5: Desktop display usage profiles

2.3.4 Mobile devices

Item	Description	Usage profile
Phone1	Basic smartphone	Entry-level smartphone with industry-standard OS, multi-touch display and integrated personal information management
Phone2	Advanced smartphone	Advanced smartphone with industry-standard OS, advanced security, multi-touch display and mobile device management support
Phone3	Ruggedised smartphone	Specialised smartphone with industry-standard OS, multi-touch display, dedicated operational use case and rugged design
Tablet1	Basic tablet	Entry-level tablet with industry-standard OS for apps, media and communications, with 7"+ colour multi-touch display

Item	Description	Usage profile
Tablet2	Advanced tablet	Advanced tablet with industry-standard OS for apps, media and communications, with 7"+ colour multi-touch display
Tablet3	Ruggedised tablet	Specialised tablet with industry-standard OS, dedicated operational use case and rugged design
PDT1	Entry-level portable data terminal	Basic handheld terminal for use in office/light industrial data capturing applications; built-in support for auto ID technologies
PDT2	Advanced portable data terminal	Advanced, ruggedised handheld terminal for use in mobile/industrial data capturing applications; built-in support for auto ID technologies
PDT3	Specialised portable data terminal	Ruggedised handheld terminal for use in specialised mobile/industrial applications; built-in hardware (e.g. sensors, communications) supporting such use cases (e.g. biometrics, 2-way radio, etc.)

Table 6: Mobile devices usage profiles

2.3.5 Device Management tools and Accessories

Item	Description	Usage profile
DevMgmt	Device management tools	Device management tools/software, offering alerts, tracking, deployment support or remote control to enable cost and labour reduction and/or value-added services for PCDs
Accessories	PCD accessories	Value-added upgrades, peripherals and accessories (incl. USB, bluetooth and PCIe devices, carry bags and locks) for use in conjunction with PCD systems

Table 7: Management and Accessories usage profiles

2.4 Bundled accessories and support

Each PCD Item is specified as a **fully working solution** with a minimum set of mandatory bundled accessories and services. For example, all computing devices are bundled with a mandatory SLA, standard OS, CPU RAM and storage, and all laptops include a carry bag and security lock by default. None of these components may be left out by suppliers, but Government may substitute the default components with alternatives or upgrades (e.g. 4GB standard RAM may be upgraded to 8GB if required.) Departments do not need to specify any components or configurations to get a working system, unless there are additional requirements (e.g. a smart card reader or upgrades to the standard support SLA).

The specification prevents suppliers from quoting or delivering incomplete solutions (e.g. PCs without Windows or laptops without carry bags), and suppliers are mandated to quote and deliver fully working solutions.

Mandatory support SLA: all devices in the PCD domain are bundled with a **3-year on-site support SLA** included as a mandatory component. To ensure the lowest possible TCO for Government, the warranty and support **cannot** be unbundled from the base unit. Due to the nature of some mobile devices, specific Items (phones, tablets and e-readers) are excepted from the 3-year requirement, and are only specified with a **1-year SLA**.

For devices with a projected longer lifespan, SITA recommends **upgrading the standard 3-year SLA** to 4 or 5 years.

2.4.1 Service delivery zones

These zones are geographical areas within South Africa where product and service delivery are required by Government. Areas are designated as Zone A, B or C, depending on proximity to large centres. Consult the Annex for geographic and turn-around time details

In addition to the 1/2/3 business-day repair time, the specifications require a **4-hour call acknowledgement**, during which period the service provider must contact the client and acknowledge receipt of the support ticket.

3. PCD selection guidelines

3.1 Principles

- Select and deploy appropriate solutions and technologies for specific business requirements (e.g. mobility or performance). Fit-for-purpose solutions enable efficiency and support cost containment.
- Business requirements and RFP/RFQ specifications must be brand- and product-independent. Specifications that contain product-specific elements will not be allowed, unless a Department-specific standard, approved by the delegated authority, is in force.
- Detail product specifications (e.g. CPU clock speed in Ghz) must **not** be used to define an end-user requirement. The **business need** must be defined based on actual usage requirements.
- The PCD domain focusses on enterprise-level devices: this means that manageability, compatibility and longevity of systems and accessories are maximised while TCO is minimised. Systems designed for a retail or home environment will not meet this requirement, and will not be certified.
- Where possible, Departments should standardise on brand and model to reduce complexity and maximise interoperability, continuity and user productivity.

3.2 Selection based on business requirement

The most important principle in deploying any ICT system, including PCDs, is that the **end-user requirement** must determine the type of system or device that must be procured. In the PCD domain, this effectively means that the device must be able to run the required software in the environment where it is required (e.g. a hand-held terminal for stock-taking).

Once the business requirement is met, secondary considerations such as additional functionality, cost, security, etc. must be factored in as well. But the primary determining factor must be the value the system will bring to the end-user’s process or function.

The basic philosophy when specifying any type of device is to procure the lowest-end system that meets all business requirements. Buying a higher-end system than what is absolutely required is not an effective use of funds that could be put to other uses.

The diagrams below break down the PCD domain into high-level category and business criteria. Standard PCs and more specialised derivatives such as thin clients and workstations are broken down into the type of work done on the systems. Newer form factors such as all-in-one PCs, ultra-small chassis and “compute sticks” can add value in environments with constrained physical space. However, the form factor is usually a secondary driver, and should only be considered once the primary computing needs have been addressed. For example, a compute stick would not be able to run advanced engineering applications, and therefore the benefits in footprint are irrelevant to an engineering user with high-end computing requirements.

New computing environments such as VDI and ChromeOS can add significant value in terms of making computing resources available to specific environments such as Education. However, as with the more traditional environments, Departments must first determine whether these devices will be able to run the applications required by their end users before deploying these platforms.

In general, a "Power user scale" can be derived from the sub-divisions: task-based user ➔ basic user ➔ advanced user ➔ knowledge worker ➔ engineer. Departments must determine where on the scale a specific user fits in order to procure the correct device. One of the distinguishing factors is the amount of content that is created or processed, vs. whether the user primarily consumes content.

3.2.1 Desktop PCs

Desktop PCs represent the most basic type of computing experience with no mobility, ruggedness or specialised connectivity requirements. As such, the selection process for a desktop PC can be applied to all other computing devices, after which the additional requirements such as mobility can be considered. The basic factors used to identify and select a desktop PC are as follows:

- Profile of user: task-based / basic / advanced / knowledge / engineering
- Applications used: web-based / network-based / local / specialised – specific or specialised apps, or apps with heavy requirements must be stipulated
- Configuration requirements of largest application: CPU, RAM, storage, connectivity
- Type of devices/categories that support the user profile and configuration requirement (e.g. PC3, PC_WS1)
- Cost elements (TCO)
- Other factors such as required functionality (e.g. dual network adapters), existing Departmental standards (brand and product)

The diagram below matches the types of desktop devices to specific use cases.

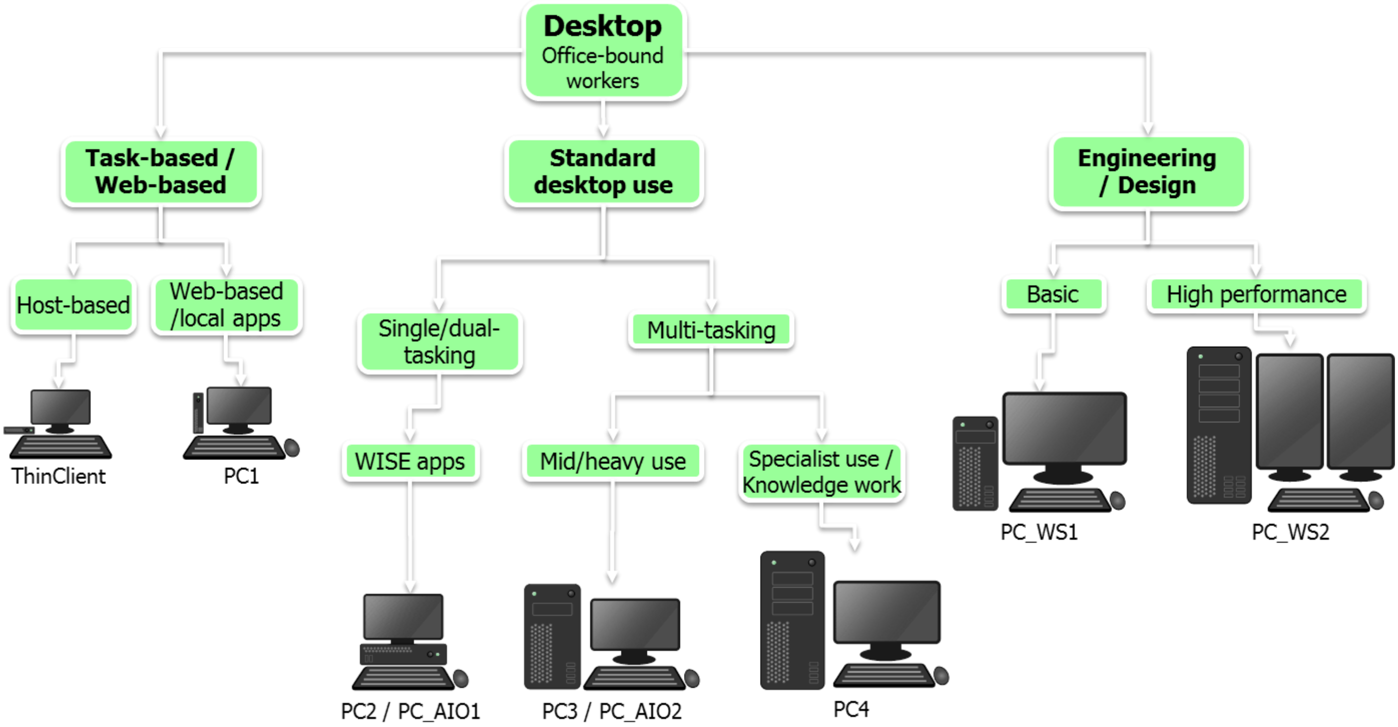


Figure 4: Desktop device decision tree

3.2.2 Mobile PCs

Portable devices are sub-divided into traditional laptops and their derivatices, and newer device types such as tablets and smartphones. The first decision needs to be the specific type of device required: standard laptop, new form factor laptop (e.g. convertible), or a tablet or smartphone. The following are the decision factors for laptops **in addition** to those used for Desktop PCs:

- ❖ Primary usage model: host-based / basic / highly mobile / knowledge worker / engineering / industrial
- ❖ Physical: maximum size and weight (often determined by user preference)
- ❖ Minimum battery life: how long must the device function away from AC power
- ❖ Additional requirements such as docking, connectivity, touch, biometrics, type of carry bag

The diagram below maps specific mobile PCD categories to broad usage profiles.

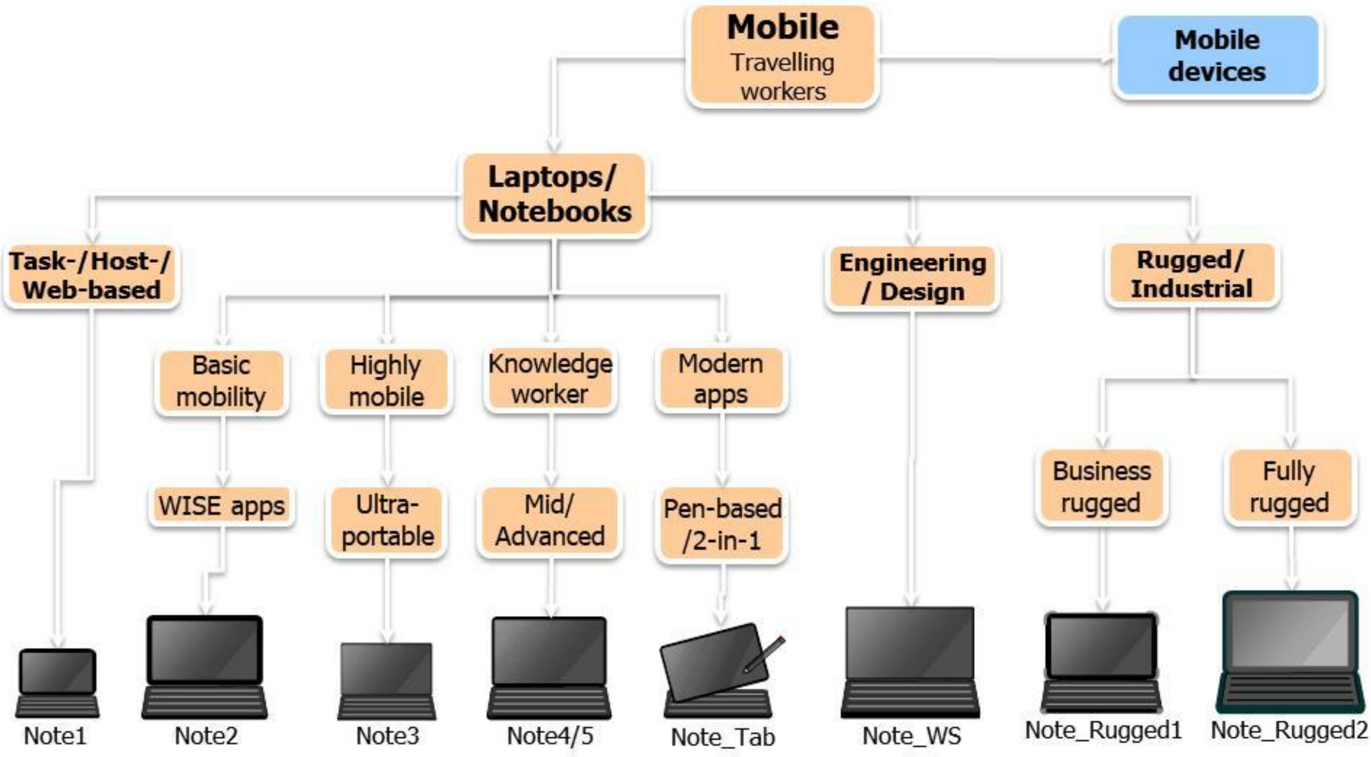


Figure 5: Mobile device decision tree: laptops

3.2.3 Desktop displays

Desktop monitors are usually deployed where a PC's bundled monitor is not sufficient, or a mobile user needs a desktop display in addition to the built-in laptop monitor. In many cases a secondary display is required by the user. Factors that determine monitor selection:

- ❖ Application requirements: type and amount of data to be displayed, as well as impact of specific used applications
- ❖ Detail requirements: resolution and screen size
- ❖ Available desktop space
- ❖ Connectivity: what type of connection does the host device have
- ❖ Ergonomics: sharpness/detail level, viewing angles, tilt/rotate functionality

3.2.4 Mobile devices

Where a standard or new form factor laptop device does not meet the user requirement, tablets, smartphones or industrial handhelds are often deployed. These devices provide a much higher level of mobility, or additional capabilities such as on-board auto-ID functionality (e.g. barcode scanner) or a design suitable for outdoor and industrial use. In addition to the factors for desktop and mobile PCs, the following factors must be considered when selecting a mobile device:

- OS and application requirements, including whether bespoke application development is required
- Environment in which the device will be used (e.g. office / stores / outdoors / hostile) and the resultant level of ruggedness of the device (e.g. IP54, 1-metre drop spec)
- Physical and geographical locations affecting network coverage (e.g. rural areas, urban environment, stores), including availability of WiFi or WWAN coverage
- How users will be using the device on a day-to-day basis
- Auto ID requirements: e.g. on-board barcode/RFID scanner
- Advanced mobility: e.g. all-day battery life, secondary/spare battery, wireless charging
- Specialised docking requirements: e.g. vehicle
- Connectivity: how and whether the device will need to connect to the network (e.g. WiFi, 3G, LTE, etc.)
- UI requirements: physical keyboard / touch / stylus / dedicated buttons for specific functions
- Specialised input requirements: e.g. signature input as part of transaction verification

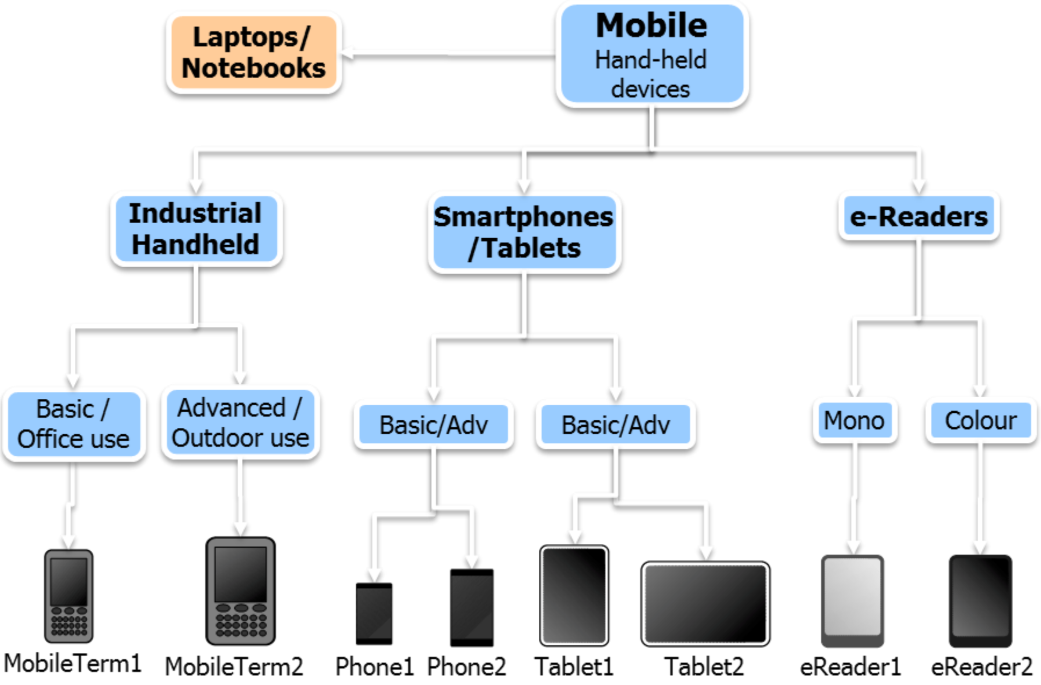


Figure 6: Mobile device decision tree: hand-held devices

3.3 Additional selection guidelines

3.3.1 Capabilities vs. price

In general, the Desktop and Mobile PC categories are arranged in ascending order of capabilities and estimated price. Both categories have several specialised capability options, such as Workstations, Tablet PCs and ruggedised laptops (Note_Rugged2). The diagrams plot the various categories on a capabilities/price graph, and also provide a relative projected sales volume indicator.

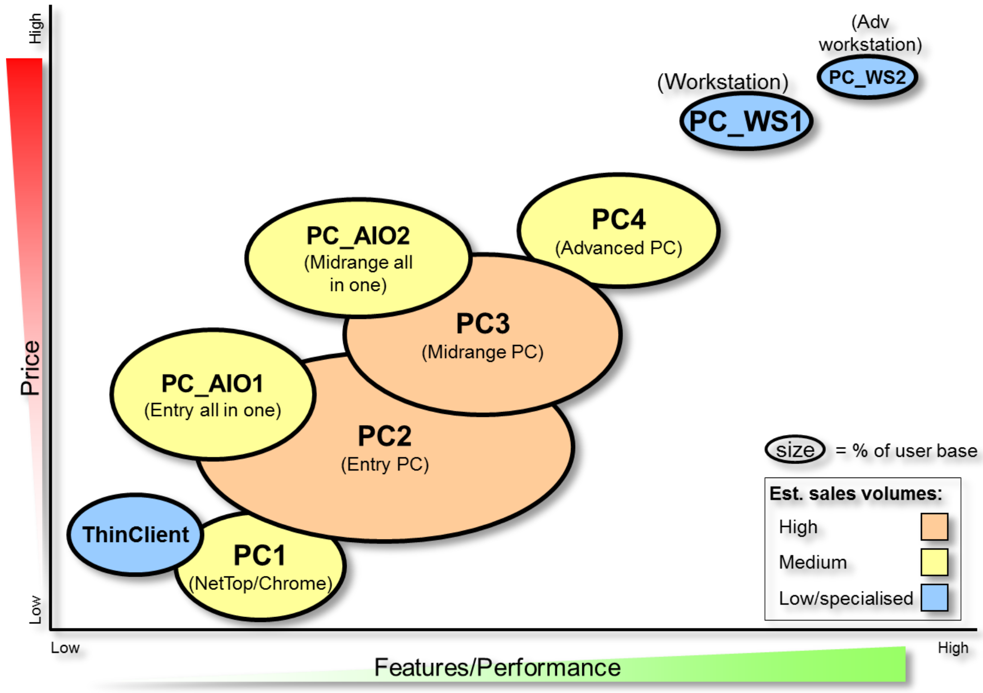


Figure 7: PC cost/capabilities overview

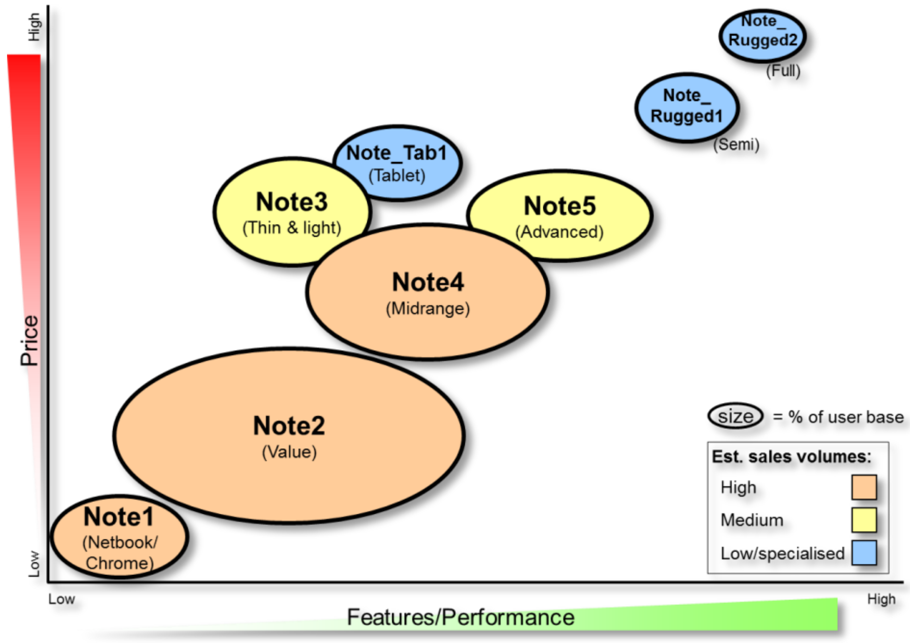


Figure 8: Notebook cost/capabilities overview

3.3.2 Considerations for ruggedised systems

Certain applications require portable PCDs to perform in extreme environments, being able to handle elements such as heat, cold, dust, moisture and physical shocks such as being dropped from height. These devices are typically specialised, and significantly more expensive to procure than standard devices. Decision factors for ruggedised systems included:

- Indoor/outdoor use (outdoor devices must typically be more rugged)
- Temperature range the device will be used in (e.g. –5 to 40˚ C)
- Impact requirements (likelihood of the device being dropped or regularly bumped during use)
- Vibration (e.g. deployment on vehicles)
- Water resistance (outdoors devices may be exposed to rain or water splashes)
- Humidity of typical environment
- Altitude (very high or low altitudes such as submarines or aircraft)
- Sand or dust protection

Ruggedised products are rated according to the IP standard, which indicates protection against water and solid intrusion into the system. Depending on the requirement, levels IP54 or IP65 should be a minimum. In addition to the IP rating, the US DOD MIL-STD tests systems in terms of temperature shock, altitude, impact, vibration and harsh environmental challenges.

3.3.3 Alternative form factors and device types

New types of end-user systems have proliferated over the past several years: devices such as ultrabooks, tablets, smartphones, zero clients and all-in-one PCs are a few examples. Departments must be aware of the benefits and pitfalls of these new form factors, as every design is typically the result of a series of compromises.

- Ultra-small form-factor PCs can save significant desktop space, and also use less power to operate. Possible expansion (RAM, disk drives and PCI cards) and connectivity requirements (available USB ports, wired network, etc.) must be considered before making the final decision.
- As with small form-factor PCs, all-in-one PCs take up less room on a desk, but they are usually less expandable or upgradeable, and may be more difficult to repair.
- Smaller and lighter laptops often have lower performance and smaller screens and keyboards, possibly impacting usability and productivity. Users should be comfortable with a laptop's screen and keyboard size in order to maximise the device's utility. Note also that features such as built-in stylus, additional ports or WWAN adapters can have an effect on the size and weight of the device. Any portable system is always a compromise, and Departments must ensure that they select the best combination of features and mobility by emphasising the must-have features over "nice-to-have" functionality.
- Tablets provide unique benefits in terms of mobility and support for a new generation of touch-based applications, but the design may compromise productivity for more traditional use cases (e.g. use with external keyboard, traditional desktop applications).
- Careful study is required when considering VDI, thin/zero clients or other host-based solutions. Factors such as back-end infrastructure, reliability of network connectivity and end-user functionality must be considered, and TCO studies must include all variables (client, server, network and projected support costs) to ensure a cost-effective solution.
- Google's ChromeOS has been gaining market share over the last few years, and in certain vertical application areas (e.g. education, browser-based workflow) ChromeOS-based devices can add

significant value. Fitting in with this trend, enterprise applications are becoming more and more web-based to allow wide deployment and client device independence. However, confidentiality of Government data and compatibility with third-party applications must be considered before making a decision.

- Thin or zero clients have been getting more attention within Government, as the deployment model (virtual desktop infrastructure, host-based computing, centralised processing) has the potential to reduce costs and management overhead. Departments must take note of the additional burden on the network and back-end infrastructure, and also compatibility of existing applications, prior to deployment. The server infrastructure and network must be fully capable of supporting the additional processing requirement of possibly 100s of client devices, or need to be upgraded before rolling out any type of thin client solution. VDI or thin-client solutions may require components from multiple transversal contracts, since a large part of the equipment that may be required is servers, storage and networking. Only partners with proven experience and credentials in deploying host-based solutions should be used to ensure a well-designed and stable solution.
- Technical and engineering workstations are a significant niche requirement in many Government departments. Where specific applications or levels of performance are required, standard PCs typically cannot meet the need. Departments need to be clear on which applications will be used, and the level of performance must be specified in order to procure appropriate workstations. Specifying ISV certification for the required application (over and above the base SITA spec) is vital to ensure support from hardware and software OEMs.

3.3.4 Ergonomics

New form factors such as tablets and smaller laptops have introduced significant change in the way they are used, and bad or unhealthy postures are often the result of struggling to read text on a small screen, or typing on a virtual keyboard. Keeping basic ergonomics principles in mind could decrease the risk of long-term health issues.

- Take frequent breaks and change your posture. Stretching is a useful activity during breaks.
- Ensure that the display is at a comfortable level; set the device on a desk or similar surface where possible. If used on a lap, sit in a comfortable chair and place the device in a comfortable position. Use accessories such as stands for laptops or monitors to adjust screen height – or make use of the built-in ergonomics of higher-end displays.
- Keep all joints (e.g. wrists) at a natural angle, and do not stress any part of the body while working. For example, a mouse should be placed on a surface large enough to support the user’s hand and forearm to reduce stress.
- Reduce glare by angling the screen to minimise reflections. This will help avoid eye strain. Other factors such distance of the screen from the eyes, text size and screen brightness must also be optimised.
- Do not carry too heavy a load; only put the most essential devices and accessories in a bag to avoid strain.
- When choosing a device, ensure that an optimum balance is maintained between weight, ergonomics and the sizes of screen and keyboard. A very small laptop may look impressive, but if you can’t comfortably work on it, get something bigger.

3.3.5 Guidelines for users with special needs (assistive solutions)

PCDs for users with disabilities or special needs (including assistive technologies) typically need to have higher-end configurations (CPU, RAM, storage, power supply) to support the higher-level computing requirements associated with supporting additional assistive software or devices.

3.3.6 Miscellaneous guidelines

- Departments must keep in mind possible additional requirements for complementary products or services, for example headsets for mobile users, web cameras for conferencing, or security devices.
- Make use of disposal services offered by OEMs for end-of-life products and used consumables.
- UPS recommendation: for environments with unstable power but no access to building clean power, a small 1kVA line-interactive UPS can be deployed to support up to 2 PCs. UPSs for this requirement are available from the PCD Accessories category.
- Enable power saving on all devices, including desktop PCs. To save electricity costs and minimise the environmental impact, devices must be set to sleep when not in use.
- Make provision for training, including establishing policies that require training and accountability to ensure that end users are able to to make full use of new capabilities offered by deployed systems. Support personnel usually also require training when new technologies are implemented.
- All networked devices must be secured as thoroughly as possible: at least the remote management interface must be password-protected to prevent attacks. All default passwords must be replaced with a complex alternative. Devices with WLAN (802.11) connectivity must be configured according to the WPA-3 security standard.
- Support is available for previous versions of operating systems, making it possible to maintain existing Departmental standards. For example, a consumer-class system is shipped with Windows Home Edition, which is not a standard for Government. For more information, refer to the Research Report on procuring systems from retail stores (see **References**).
- Headsets can increase productivity for users in mobile or open-plan environments: Departments should determine whether wired or wireless is required based on user profile. Features such as noise cancelling and UC certification should also be considered and balanced against increased cost.

4. Engagement guidelines

The Personal Computing Devices domain specifies minimum requirements in terms of service delivery, security, maximum repair times, etc. Clients and suppliers are urged to familiarise themselves with these requirements in terms of their respective rights and responsibilities.

4.1 Department guidelines

As detailed as the SITA certification process is, it cannot measure individual client requirements without including variables applicable to specific Departmental scenarios. By definition, this cannot be done in a transversal initiative, as the specification caters for all of Government for a multi-year period (typically). Therefore, a process must be followed to specify and select the best solution for specific client needs. SITA TAS can provide additional data and a consultation service to develop the criteria for a Departmental evaluation.

To ensure an open and fair process, the process may not favour any brand, product or supplier. An exception to this rule is where Departmental standards are used to lower TCO, as recommended elsewhere.

Departments are encouraged to use the following guidelines and variables in specifying solutions. Clauses that must be included in requests are included in **Annex A** for reference. These are normative guidelines, and as such **must** be followed by Departments making use of transversal contracts.

4.1.1 Business requirements

Before procuring and implementing any solution, Departments must define how, where and for what it will be used for. The functional requirement must be stated up-front as part of the procurement process. A detailed list of considerations is provided below.

- Business requirements, not technology, must drive ICT acquisitions. This is to ensure that costs are contained and specific business needs are met. All business requirements must be specified up front, including a functional description of the required solution, including for example monthly volumes, deployment environment, etc.
- Departments are not allowed to use specifications provided by suppliers when publishing a requirement. The specification must defined based on actual business needs.
- Government offices are located all over South Africa, and provision has been made for localised service delivery. Departments must stipulate the required locations of service provision to determine which suppliers can provide support to the client. The zones of service delivery must be taken into account during this process. E.g. if a Department requires service delivery in the Eastern Cape, only suppliers with a direct presence in that province should be considered.
- For complete solutions, the request should cover at least the following elements:
- An overview of the solution and a high-level list of components, including which of the existing infrastructure and components would need to be upgraded or replaced.
- Installation and configuration of complete solution.
- Integration into existing infrastructure and functionality.
- Commissioning of system and formal acceptance by client of a complete working solution.
- Training of user’s operational staff for day-to-day running of system.
- Support of entire solution, including warranty and maintenance. An SLA should be defined up front in the RFQ.
- Required warranty, maintenance and support for the solution (both preventative and reactive).
- Possible future upgrades with open standards-based interfaces.
- Future-proofing of the required solution must be planned for to ensure the maximum value for the investment, as well as to guarantee interoperability with future technologies and protocols.
- Selection of the most suitable alternative must based on the lowest TCO calculated using the user requirement as input.
- Departmental standards should be used to expedite procurement of approved devices, while only exceptions (deviations from the standard) need to be explicitly motivated and approved by internal ICT committees.

4.1.2 Sizing and performance of solutions

- As with reliability and performance, the configuration and operational parameters of a system largely determine TCO, or cost-effectiveness. Capital costs and on-going costs (consumables, service, support, etc.) vary widely based on many factors. Licensing costs for additional required functionality (e.g. additional software functionality) must also be calculated. All these factors must be incorporated in the requirement to ensure a real-world comparison of total cost. Clients are encouraged to do a multi-year TCO comparison (a minimum of 3 years) as part of the process.
- Sizing of solutions must take into account actual business needs, including all requirements and variables such as document volumes or mobility requirements. Guidelines from integrators, software

developers and OEMs must be used to specify the solution and required performance. Existing and planned network infrastructure must also be taken into account when specifying the solution.

- System configuration, including component specifications such as connectivity and capabilities needs to be correctly specified based on end-user requirements.
- When proposing a solution, suppliers must provide a complete list of all SITA-certified Items. This is addressed in detail later in the document.

4.1.3 Service and support

- Service and support requirements must be addressed thoroughly by the client via service level agreements (SLAs). For more complex or mission-critical solutions, upgraded SLAs must be specified and negotiated as part of the procurement process.
- Detailed support and maintenance requirements must be stipulated up front as part of the specification.
- Up-to-date certification of service providers is vital to maintain OEM warranties: technician certification for some OEM products have to be renewed annually.
- Most OEMs commit to supporting a product for at least 3–5 years after being discontinued. Government can partly address this concern by opting for a more comprehensive SLA up front.
- Countrywide delivery is included as a mandatory component in all technology domains. Required delivery times must be negotiated with the supplier, and non-performance can be managed by involving the appropriate SITA resources. Delivery and/or installation of complex solutions or systems must be project-managed in conjunction with the supplier or solution architect.
- Changes to any ICT infrastructure (e.g. network or server configuration) should only be done by certified resources, whether internal or contracted. This will ensure that all changes are done in a controlled way, and system reliability is maintained.
- To ensure maximum reliability, integration and functionality, Departments are urged to procure solutions from a single supplier or consortium instead of buying different components from different suppliers. A single point of contact (call centre) must be established at the supplier for all maintenance and support.
- In order to ensure data security, Departments must ensure that devices that are being disposed of have their storage media securely erased as per the guidelines elsewhere in this document. In addition to this, if a device has to be replaced or taken offsite for repairs, the storage medium (e.g. hard drive) must remain in the Department’s possession, not removed with the device.

4.2 Supplier guidelines

Where applicable, certified suppliers are required to adhere to the following normative standards when supplying products certified via the Personal Computing Devices domain:

- All SITA-specified accessories, as well as any upgrades ordered as part of the solution **must be installed and fully operational** at delivery, and must be covered by the specified SLA.
- The final responsibility for a working solution rests with suppliers and OEMs. An incomplete specification by Government does not absolve suppliers of this mandate. However, if Departments specify a detailed bill of materials, or prescribes to industry in other inappropriate ways, this responsbility reverts back to the client.
- Suppliers must ensure that all required information is gathered from Departments before quoting for or delivering a solution. This is to ensure that Government’s business needs are met by the proposed solution, and that only complete solutions are offered.

- Suppliers must recommend that Departments negotiate SLAs over and above minimum uptime specifications for mission-critical systems.
- Suppliers must inform Departments of best practices in terms of deployment, SLAs and operations.
- Suppliers must commit to only proposing suitable and appropriate solutions given Government's business requirements.
- Only certified products and services may be offered to Government via the Personal Computing Devices domain, as stipulated in the SITA Act and NT regulations.
- Suppliers must be certified to supply, install, support and maintain each individual product in the solution offered to Government.
- Registration of all product warranties must be done by the supplier after delivery of a solution. Government will not be required to register products for warranty to be eligible for warranty claims and support as per domain conditions.

4.2.1 OEM responsibilities

SITA has concluded an MoA (Memorandum of Agreement) with more than 160 OEMs at the time of writing. The MoA commits manufacturers to a mandatory level of support, quality and development of local industry. OEMs participating in the product certification process have the following responsibilities:

- Take primary responsibility for the entire technical evaluation process (product certification), including informing partners of progress if required.
- Participate in the technology management process as per domain conditions (refer to **Technology Certification Process,** and **OEM Memorandum of Agreement**)
- Ensure that appropriate, suitable solutions are offered to Government based on the stated business requirements.
- Take responsibility to determine the appropriate parts required to build a working solution, and communicate this to all OEM partners.
- Support all their partners in terms of certification, training and regional service provision.
- Provide all required information to SITA, such as technical details and product roadmaps.
- Ensure that all partners supplying the OEM's products will adhere fully to the technical spec and solution requirements, either via training, management systems or auditing.
- Ensure that the optimal configuration for the stated user requirement is delivered by suppliers.
- Maintain the certified product database, ensuring that all products listed are current, and updating those that have been replaced or superseded.
- Restrict the number of configurations of a specific product offered by all suppliers to a single configuration (i.e. that a single configuration of a particular model will be offered by all suppliers). SITA will engage the OEM during the process in support of this goal.

If the supplier fails to perform according to specification, the accountability will devolve onto the OEM automatically. Failure to comply with these guidelines will result in corrective action by SITA.

4.3 RFQ process

A critical procurement principle is that Departments are not allowed to use specifications provided by suppliers when publishing an RFQ. The requirement needs to be defined based on actual business needs.

The following high-level procedure should be followed when engaging suppliers:

- Ensure that all applicable guidelines in this Deployment Guide are followed.
- Determine and **document detail requirements** (see guidelines and requirements sections for specific information around this).
- Verify **appropriate sizing** of requirement before publication.
- Approach SITA for **advice** (if required).
- A bill of materials may **not** be specified, as this places the burden of a working solution on Departments, instead of bidders.
- Domain Item names (e.g. PC3, Note5, Tablet1) may **not** be specified to clarify the requirement, since this prevents bidders from offering similar or superior alternatives.
- As discussed earlier, define a list of **evaluatable**, mandatory business criteria to be included with the RFQ. This includes for example requirements for additional components (e.g. docks, high-end monitors or extra storage), services such as regional delivery, installation and maintenance, or upgrades from the base specification to meet additional performance requirements.
- **Publish request** with documented requirement. All information about requirements, infrastructure, constraints, etc. must be shared with all respondents, i.e. if new information becomes available during adjudication, all respondents must be allowed to update their responses. Any requirement not stipulated up front may not be used to adjudicate bid.
- Suppliers may only quote solution components, equipment, accessories and upgrades that were listed in the product detail specification at certification. This is to ensure that the solution is made up only of certified components.
- Evaluate RFQ in terms of TCO, supplier TCO, BEE and compliance with requirements (technical). The **PPPFA 90/10 principle** must be utilised in this process. Departments are encouraged to tailor TCO calculations for their specific environment. It is important to verify during the technical evaluation that **all mandatory components** (e.g. 3-year support) are included in the quoted price, using the submitted bill of materials or pricelist. This is to ensure a fair, apples-to-apples cost comparison.
- Award to the most **suitable bidder**, i.e. the one with the highest-scoring bid that complies with all requirements.

The Engagement Model has more details on this process.

4.4 Solution and supplier selection

The following criteria must be considered when selecting a product and supplier:

- The OEM, supplier and product need to meet the requirements shown in the Venn diagram: only solutions in the white intersection may be considered for selection.
- The supplier must meet the following requirements before their bids can be considered:
  - Certified to supply products via the appropriate contract (information on the SITA website can be used to verify this).
  - Certified to supply the required product Category and Item.
  - Certified in the province where the solution must be delivered/installed.
  - Certified by the OEM to supply the specific products offered in the request (filtering of information published on SITA's website can be used to verify this).

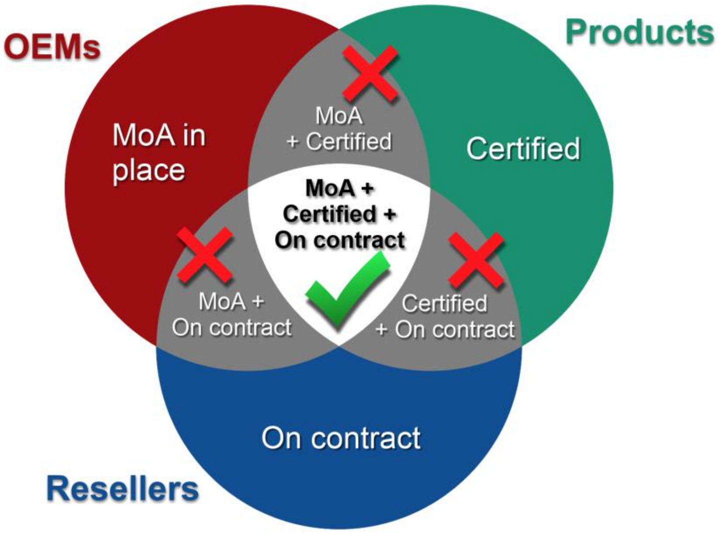


Figure 9: Requirements for supply to Government

- The supplier must be capable of providing, commissioning and maintaining a solution of the required scale.
- The offered solution (both technology and scope) must meet the client's business needs.
- Certification of products and resources (solution-level, OEM-level, skills-level, etc.) for specific platforms and applications.
- Client's current installed base: moving to a new supplier and/or product range may increase TCO by impacting on existing certifications, training, logistics and compatibility.
- Supplier track record and relationship.
- Support for and understanding of client's unique requirements.
- Service issues such as delivery and repair times.
- Other soft issues (support footprint, regional distribution, etc.). Provincial goals may be incorporated here as part of the 90/10 principle.

5. Services, best practice and deployment guidelines

5.1 Technology management

This section provides an overview of the processes and services performed by SITA . This includes the following technology and contract management processes:

- Tech updates (including structural changes such as new categories, and moving products between categories). Tech updates are done periodically depending on Government requirements. The latest update is always available at the SITA Certification website (www.sita.co.za/prodcert.htm).
- Model changes and the introduction of new products, categories or items.
- Contract/technology refresh: a regular process allowing additions of new technologies, products and suppliers.
- Removal of duplication between technology domains

- Dispute resolution
- Consultation to Departments

5.2 Deployment of technology

This section provides an overview on best practices in terms of deploying solutions from the Personal Computing Devices domain. As most of these solutions offer significant capabilities and capacity, care should be taken to have the correct implementation framework in place.

5.2.1 Policies and/or strategies

The following policies and/or strategies should be in place to inform business practices, technology requirements and procurement initiatives:

- Security policy in terms of information and physical access control
- Information management policies and strategies:
    - Data management policy
    - Storage and backup strategy, policy and procedures
    - Archival policy
- Disaster recovery (DR) policy and strategy
- Infrastructure management policy
- Support strategy
- Maintenance strategy:
    - Ceding of warranty to in-house service providers may be done at purchase time, depending on existing agreements that Departments have in place.
    - Transfer of maintenance contracts should be done to in-house service providers after the standard 3-year warranty expires.

5.2.2 Deploying Windows 11

Windows 11 is the latest *de facto* desktop operating system in Government, but it needs to be approached with caution to ensure that the transition from Windows 10 or older versions of Windows is as smooth as possible.

- Plan for Windows 11 adoption as soon as possible, since Microsoft, industry and technology are forcing a move away from Windows 10. New PC hardware being launched into the market no longer supports Windows 10, so Departments have to plan to move to the newer OS in a controlled way.
- Develop a project plan for rolling out the new OS.
- Note that newer hardware (e.g. Intel Gen12 processors and later) will have limited or no support for Windows 10, and therefore migration is inevitable in the short to medium term.
- Test business-critical applications and system on new OS and browsers.
- Also test less critical software to measure migration impact.
- Phase in Windows 11 with new PCs to minimise hardware compatibility issues.
- Manage automatic OS updates carefully to minimise disruption.

Departments are encouraged to study the TAS research report on desktop Windows security and optimisation, which can be found in the References section.

5.2.3 Open-source software options

One of the most basic strategies for any ICT organisation is to avoid being locked into a particular system, format or vendor. This provides the organisation the freedom to migrate away from problematic systems or vendors, or towards an environment that offers superior functionality, security or cost-effectiveness. With Microsoft's OS, infrastructure and applications suite having been the *de facto* standard for so long in Government (and worldwide), questions often arise about the possibility to move away from Windows, Office or Exchange.

In support of this strategy, SITA has ensured that all certified desktop and mobile PCs support an alternative FOSS operating system, nl. Linux, for at least a decade. Peripherals were certified against the same requirement where appropriate. This is to allow Departments the option, should the opportunity arise in future, to migrate away from Windows without having to replace any hardware.

Unfortunately there are a lot of caveats, risks and complexities involved in replacing any major piece of software that Government has become dependent on over a period of several decades. Data formats, application interfaces, software compatibility and end-user training are some considerations that need to be addressed thoroughly before any decision to migrate can be made.

As background, we need to be aware of the fact that Microsoft (and most other vendors) actively work towards locking their customers into their formats, systems or broader ecosystem. Over many years Microsoft has used Windows, Office and Internet Explorer, among others, as leverage to extend their control over customers' ICT environments. This is of course a basic strategy for any supplier who wishes to maximise revenue. Conversely, we as customers should resist that strategy by ensuring that we are able to move away from any incumbent vendor should the need arise.

With the advent of cloud technologies, vendors now have unprecedented potential for control over their customers – to the extent of storing users' data and being able to refuse access if the client stops paying for the service. This is a frightening scenario that Government can very easily find itself in: if our data is stored in any non-Government cloud, what guarantee do we have of security, unrestricted access and data integrity? Moreover, if all our communications (video calls, e-mail and unfied communications) transit the public internet to and from an overseas-based cloud service, how secure are they? The issues of information security and data sovereignty are only peripherally related to open-source software, and is therefore beyond the scope of this document.

The most well-known alternatives to Microsoft products are usually open-source offerings such as Linux or LibreOffice, being possible replacements of the 2 most widely-used products in Government, nl. Windows and Office. Both these products are very mature and functional, and are used widely across the world by a broad range of organisations with little or no issues. However, given that Microsoft deliberately makes it difficult to migrate, there are significant complexities with starting to use these products within Government.

These complexities include hardware and software compatibility, document conversion issues, training users on unfamiliar interfaces, and integration into existing services such as overseas cloud applications.

We recommend that Departments seriously consider Microsoft alternatives on a regular basis in order to avoid being locked into an ecosystem that will keep on expanding until it uses up the entire Government ICT budget.

5.2.4 Guidelines on Apple devices

TAS, Government CIOs and supply chain officials regularly receive requests from their clients or users for specific Apple devices, e.g. MacBooks or iPads. After extensive discussions within the GITOC TTT, the following observations, operational issues and risks were identified:

- Apple MacBook Laptops (e.g. MacBook Air or MacBook Pro) are used by some executive managers as well as for scientific research purposes, specifically using analytical and numerical modelling software (e.g. MatLab).
- Use of Macs for research purposes including analytical and numerical modelling has proved to be more efficient and higher performing than equivalent "Wintel" models. However, note that the Apple Mac systems are considerably more expensive than a typical mainstream PC equivalent.
- At present the warranty and SLA for Apple devices are **not** on-site as is with standard Windows-based equivalent devices. An extended warranty is available (iCare) in addition to the standard 1 year carry-in warranty, but this must be registered within a few days of delivery otherwise it is a wasted expense (TBC). The Apple Warranty is a carry-in service, meaning the user must take a faulty unit into the nearest iStore for repair. The turnaround time for the warranty repair is anything from 2–21 working says with no loan units provided. This means that potentially, an executive (DG/DDG, etc) may be without a laptop if their MacBook "breaks" for more than 3 weeks. The units on RFB 740 come with a Next Business Day on-site warranty. SITA is engaging with Apple at present, and once they are on board this service option will conform to SITA's standard on-site SLA requirements.
- Apple devices are difficult to integrate into Active Directory: for example, some Government users have passwords set never to expire, which this creates a huge technical risk as well as a potential major security audit finding.
- Enterprise anti-virus software does not seem to work optimally on Apple devices. Government uses MS Defender and Trend Endpoint Protection, as examples, but for Apple laptops 3rd-party free AV software has to be used – this again presents significant risks.
- Despite some technical staff having access to MacBook units, technical support remains a challenge with junior staff not having the capabilities nor the confidence to support executive-level MacBook users on a regular basis.
- Desktop Publishing (DTP) and design-oriented groups within Government often use Apple systems (iMac, MacBook, Mac Pro) that have been proven to have superior performance in this area over the traditional "Wintel" technology. Unfortunately Macs configured for the required performance are typically prohibitively expensive (>R60k – R80k per unit). The useful life, warranty and availability of support and spares remain a challenge despite the proven performance of this technology in this space.
- Many requests for MacBooks come from users whose primary requirement is for administrative functions, not a unique requirement for Apple technology. Some request Apple devices to integrate with their iPhones and iPads, which does not make sense from a corporate perspective, as this is a personal preference. Again the issue of costs is also a challenge as this is definitely more expensive than equivalent PC models.
- There is a phenomenon within the broader ICT community, and also within Government, to procure Apple devices (e.g. iPads, MacBooks, iMacs) based on their "cool factor" or superior design, and not based on a genuine business requirement. This can result in wasteful expenditure, since Apple devices are usually significantly more expensive to buy, and usually do not fit into standard device management and security frameworks to reduce risk and lower operational costs.

SITA would like to express thanks to DFFE officials who contributed the bulk of the observations in this section.

Recommendations for deploying Apple devices

Given the above risks and operational difficulties caused by Apple systems, and based on consultation with industry and client bodies (including GITOC TTT), the following is recommended w.r.t. Apple devices:

- Only procure Apple devices where there is a genuine business need (i.e. an application or system that only runs on MacOS or iOS).
- Make end-users aware of the cost differences between standard Windows-based hardware and Apple devices.
- Specialised users or aplications (e.g. marketing, communications, graphic design) have often in the past required MacOS systems, and SITA has always supported Departments in procuring these. Departments are welcome to contact TAS for advice and support in motivating, specifying and recommending these devices.
- Establish a capability within the environment to support Apple devices, since it is a completely different (and incompatible) system architecture, OS and application stack when compared to the standard Windows or even Linux-based environments.

5.2.5 Guidelines for mission-critical systems

- Maintenance and support SLAs must be entered into for specific response/repair times and uptime for entire system, not just hardware.
- Downtime intervals should be scheduled for preventative maintenance on all equipment to ensure optimum functioning.
- The call/failure escalation procedure for each solution should be followed when downtime occurs. The procedure must be visible to operational staff to ensure quick response in case of failures.
- All OEM-provided fixes, patches, updates and alerts (affecting hardware, firmware and software) should be acted upon and implemented as recommended to ensure the best possible availability and reliability from the systems.

5.2.6 Additional best practices

- FOSS operating systems and environments are supported by all products as approved via the technology certification process, and are available preloaded with all mainstream PCs or laptops. Departments are encouraged to make use of this option where required.
- Certification of solutions to be interoperable with third-party solutions (e.g. a scanner certified by a software vendor) needs to be taken into account during the RFQ process. Departments run the risk of losing certification when selecting non-supported configurations, which could seriously impact system reliability and a Department’s recourse in case of failures. The recommendation is therefore that the entire existing infrastructure be stipulated as part of the RFQ process to enable suppliers to offer a suitable solution. In some cases a qualification process may have to be done before a solution can be certified as “supported”.
- Installation services are available at additional cost for each Item. It is highly recommended that Departments make use of these services for complex solutions, specialised devices, or where in-house skills are not available. If required, these services must be requested in the RFQ.
- SSA guidelines must be followed in terms of data protection w.r.t. storage devices (e.g. hard disk drives) at disposal or when failures occur. In general, storage devices containing Government data may not be removed from Government premises under any circumstances. Erased disk drives or portable media must be certified to be securely erased before they may be removed from

Government premises. Hard disks must be erased to at least the **US DoD 5220.22-M** standard, or an alternative security level acceptable to the Department.

- Select appropriate solutions for specific requirements. At the lower end where the risk is less, low-cost products are adequate for Government's requirements. Conversely, at the higher end, higher-priced products are required to satisfy Government's reliability requirements.
- Note that the OEM warranty usually **excludes accidental or user damage** (e.g. dropping a laptop down the stairs). Any failures not directly caused by faulty materials or workmanship are typically not covered by the warranty. Departments must carefully note what is covered by the device warranty when putting a system into production.
- In order to facilitate asset and financial management, technology solutions that control, track and trace devices should be considered as an add-on service. This includes printer fleet management solutions or hardware tracking technology for mobile devices.
- Departments must ensure that all supplied cables conform to the relevant industry standards to ensure safety and compatibility. E.g. USB cables must be certified by the USB Implementers Forum (http://usb.org). Departments should not purchase "cheap" or counterfeit cables that are not certified, since these can damage expensive devices. Poor-quality cables delivered by OEM-approved suppliers will be the responsibility of the supplier or OEM (including resolving any issues caused by these cables), unless Departments used cables not approved by the OEM.

6. Conclusion

The Personal Computing Devices technology domain supports the establishment of a transversal procurement vehicle for a baseline technology platform that should cater for at least 90% of Government's PCD requirements. Following the guidelines in this document should enable Government to make use of this domain to its maximum potential in supporting Departmental ICT and service delivery goals.

A thorough analysis of user requirements must be done to ensure that a fit-to-purpose solution is procured from the Personal Computing Devices domain. SITA can assist Government in this analysis with advice, guidelines and focussed cost models.

SITA is committed to supporting Government in its procurement initiatives by ensuring that domain and contract conditions are maintained, and Department technology requirements are met by continually revisiting the specifications and making adjustments where required. SITA's emphasis on the technology aspects enables Departments to focus on their business requirements and the value they can derive from a particular solution. Any inputs in this regard may be forwarded to SITA using the contact details provided below, or escalated via other channels (e.g. TTT, GITO Council, SITA Account Managers).

Lastly, many individuals and organisations have contributed to this document, and TAS aim to keep updating it with useful information. Any suggestions or additions to the document may be directed to the authors for consideration.

Standards, technical documents and contact details

The latest technical information, specifications, forms, and the latest version of this and other documents can be downloaded from the SITA Product Certification web page: www.sita.co.za/prodcert.htm

TAS contacts for product certification, advisory services and technology domain information:

Name	Role	Contact details
Deon Nel	Technology consultation and certification	deon.nel@sita.co.za 012 482 2136
Izak de Villiers	Technology consultation and certification	izak.devilliers@sita.co.za 012 482 2749
Hlengiwe Mosokotso	Certification requests, Lab coordination and communication	tas@sita.co.za 012 482 3333

Annex A: Sample RFP/RFQ Clauses

This Annex provides standard clauses that Government users must include in their RFPs/RFQs to ensure that specific technical and contractual requirements are met in terms of the transversal process.

Using a standard RFP/RFQ template as a basis, the following information must be inserted into the Technical/Solution part of the RFQ, which defines the specification for which suppliers must quote.

MANDATORY	Comply	Do not comply
Bidder commits to implement and follow all conditions and specifications as defined by the contract framework. This includes all technical and solution requirements listed in the transversal bid document, all requirements in this RFP/RFQ, and the latest technical product specifications. No services, features or capabilities listed as "standard" (included in the price) in the bid and technical specifications (e.g. on-site support SLA) may be excluded from the RFP/RFQ, and no RFP/RFQ conditions may override or cancel out any bid conditions or specifications.		

MANDATORY	Comply	Do not comply
The responsibility for delivering a complete, working solution will reside with the Supplier, not the end user. The Supplier will be fully accountable for the system configuration and correct implementation, notwithstanding any possible shortcomings in the specifications or RFP/RFQ. The relevant OEMs must fully support Suppliers in delivering working solutions to Government. The Supplier will be accountable for the final solution, service and support.		

MANDATORY	Comply	Do not comply
Bidder must be certified by SITA as a supplier approved on the relevant transversal contract (i.e. Contract 740).		
Substantiate: Attach proof that bidder is approved by SITA for this contract.		

MANDATORY	Comply	Do not comply
Regional applicability: Bidder must be certified on the relevant contract for product supply and service delivery (as applicable) in the province where the solution must be delivered/installed.		
Substantiate: Attach proof that bidder is approved by SITA for this region.		

MANDATORY	Comply	Do not comply
Bidder is certified by SITA to supply the proposed product brand, Category (e.g. PCs or Notebooks), Item (e.g. PC1) and specific product offered in the proposal/quotation.		
Substantiate: Attach proof that bidder is approved by SITA for this Brand, Category and Item.		

MANDATORY	Comply	Do not comply
The bidder will supply only SITA-certified products for this bid, i.e. products that are listed on the SITA product database. Supply of non-certified products will constitute a breach of contract, and will result in punitive measures. The individual product certificates for the offered products must be attached to this bid.		
Substantiate: Attach all relevant product certificates.		

MANDATORY	Comply	Do not comply
Bidder is certified by OEM to supply the specific products offered in the RFP/RFQ.		
Substantiate: Attach proof of OEM certification.		

MANDATORY	Comply	Do not comply
All major parts and components that form part of the solution must be quoted separately in the pricing schedule.		
Substantiate: Pricing schedule must be completed with individual pricing for each mandatory component.		

MANDATORY	Comply	Do not comply
Stipulate how supplier skills and experience will be evaluated (e.g. list of clients, reference sites, years of operation)		
Substantiate: Attach documents proving required criteria.		

MANDATORY	Comply	Do not comply
Design, project plan and bill of materials (BOM) must be delivered as part of RFP response		
Substantiate:		

MANDATORY	Comply	Do not comply
All additional accessories specified by the client must be included in the quoted price. If not included, suppliers will be required to supply these accessories at no cost to the client.		
Substantiate: Quoted pricing must include specified accessories.		

PRICING SCHEDULE

The only changes made to the standard SITA pricing schedule is that the schedule allows for domain-related Item and Line numbers. Please ensure that only approved products are supplied in terms of the Personal Computing Devices domain.

Major solution components	Quantity	Unit Price (Excl VAT)	Nett Price (Excl VAT)
Basic device as specified			
Basic software (e.g. OS)			
Upgrades (e.g. RAM, storage, display)			
Accessories (e.g. carry bag, dock)			
Additional software			
Additional services (e.g. optimisation, integration, software installation, data migration)			
Additional logistics (e.g. regional delivery and installation)			
…			
…			
…			
Standard SLA			
Upgraded SLA (e.g. 5-year warranty)			
		Subtotal	
		VAT 14%	
		Total VAT Incl.	

Annex B: Technology Domain Details and Technical Specifications

All information regarding the Items and Categories established via the Technology Certification Process is available as part of the detail technical specifications. Categories, Items and specifications will change as the domain and end-user requirements evolve. This information, as well as the latest Tech Update and detail technical specifications can be downloaded from the SITA Product Certification web page at www.sita.co.za/prodcert.htm.

Bundled and Optional Accessories

A general list of accessories that **must** be delivered as part of any PCD solution is provided below. Any additional accessories, services or components must be addressed in the RFP/RFQ, and included in the solution scope by the supplier.

Accessories, components and services that must typically be bundled to ensure a complete, fully working solution according to the client's requirements and standards include:

- All required power and signal cables
- Any component required for proper functioning of the system or a component (e.g. operating system and storage in a laptop)
- All interfaces required by the specified solution
- Batteries (if applicable)
- Any software application or driver required for proper functioning of the system or a component
- Standard warranty and SLA as specified
- Proper design and planning of the solution
- On-site delivery

Optional accessories and components that must be stipulated by the client or proposed by the supplier:

- Upgrades to the base system
- Additional functions or upgrades of functionality (e.g. resolution, storage, connectivity)
- Additional services such as consultation, advanced training or operations
- Migration of data from previous system
- Installation of additional software or functionality not included in the primary solution
- Any other component, accessory, upgrade or service not specified in the PCD Technical Specifications at www.sita.co.za/prodcert.htm.

Annex C: Solution Checklist: PCDs

This annex specifies the bundled and optional accessories for the PCD domain in the form of a checklist to be used by Departments to help specify PCD solutions, and determine whether a complete solution has been delivered as specified by SITA during the Technology Certification Process.

OEMs and suppliers commit to these conditions and specifications in Transversal Contracts 740, and end-users **must ensure** that solutions are delivered as specified to prevent additional or fruitless expenditure.

The checklist details all bundled components and accessories (included with Base Price) per category, as well as upgrades and options that can be specified by the client over and above the default.

Desktop PCs	
Included with Base Unit	**Not Included with Base Unit** (client to specify)
❖ Base unit with capabilities as specified in Section 1 of the technical specification ❖ 3-year on-site SLA with next business day repair ❖ CPU, RAM, hard drive ❖ Network interface (LAN) ❖ Monitor, keyboard and mouse as specified ❖ Standard power and interface cables ❖ Software: ➢ Desktop operating system (Windows 10 Pro) ➢ Drivers for all subsystems for standard operating systems ➢ Recovery mechanism ❖ Documentation ❖ Packaging and delivery to client site	❖ On-site installation ❖ Optical drive ❖ Upgrades to CPU, RAM, hard drive, graphics card, monitor, etc. ❖ SLA upgrades (beyond default 3-year on-site) ❖ Non-standard accessories, e.g. case lock, speakers, fingerprint or card reader

Mobile PCs (notebooks and laptops)	
Included with Base Unit	**Not Included with Base Unit** (client to specify)
❖ Base unit with capabilities as specified in Section 1 of the technical specification ❖ 3-year on-site SLA with next business day repair ❖ CPU, RAM, hard drive ❖ Network interface (WLAN, Bluetooth) ❖ Built-in display, keyboard and pointing device as specified ❖ Standard power and interface cables ❖ Carry case ❖ Kensington-type cable lock ❖ Software: ➢ Desktop operating system (Windows 10 Pro) ➢ Drivers for all subsystems for standard operating systems ➢ Recovery mechanism	❖ On-site installation ❖ Optical drive ❖ Upgrades to CPU, RAM, hard drive, graphics card, monitor, etc. ❖ SLA upgrades (beyond default 3-year on-site) ❖ Non-standard accessories, e.g. webcam, speakers, fingerprint or card reader

Mobile PCs (notebooks and laptops)	
❖ Documentation ❖ Packaging and delivery to client site	

Desktop Displays	
Included with Base Unit	**Not Included with Base Unit** (client to specify)
❖ Base unit with capabilities as specified in Section 1 of the technical specification ❖ 3-year on-site SLA with next business day repair ❖ Standard power and interface cables ❖ Documentation ❖ Drivers for standard operating systems ❖ Packaging and delivery to client site	❖ On-site installation ❖ SLA upgrades (beyond default 3-year on-site) ❖ Non-standard accessories, e.g. monitor stand, additional signal cables, etc.

Mobile Devices	
Included with Base Unit	**Not Included with Base Unit** (client to specify)
❖ Base unit with capabilities as specified in Section 1 of the technical specification ❖ 1-year on-site SLA with next business day repair ❖ Standard power/charging and interface cables ❖ Battery and accessories as specified ❖ Mobile operating system (Android or iOS) ❖ Carry bag or screen cover ❖ Documentation ❖ Drivers and supporting software for standard operating systems (if applicable) ❖ Packaging and delivery to client site	❖ On-site installation ❖ SLA upgrades (beyond default 3-year on-site) ❖ Non-standard accessories, e.g. additional interfaces, chargers, cases, software, batteries, etc.

All components, accessories, upgrades and services are specified in the PCD Technical Specifications at www.sita.co.za/prodcert.htm.

Annex D: Abbreviations, Terms and Definitions

Abbreviations

AIO	All In One device
AV	Audiovisual
AVCT	Audiovisual Communications Technology
BEE	Black Economic Empowerment as defined by Act 5 of 2000.
CAD	Computer-Aided Design
DP	DisplayPort
DVD	Digital Versatile Disc
ECM	Electronic Content Management
EIS	Executive Information Systems
FOSS	Free and Open Source Software
GIS	Geographical Information Systems
GITOC	Government IT Officers Council
HDMI	High Definition Multimedia Interface
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IpvX	Internet Protocol version (e.g. IPv6)
ISO	International Standards Organisation
ISV	Independent Software Vendor
IT	Information Technology
LAN	Local Area Network
LCD	Liquid Crystal Display
MIOS	Minimum Interoperability Standards
MISS	Minimum Information Security Standards
MoA	Memorandum of Agreement
MTBF	Mean Time Before Failure: measured for entire system with all mandatory components
MTTR	Mean Time To Repair: measured with engineer on-site with spares in-hand; swap-out also acceptable
NIPP	National Industrial Participation Programme
NIST	National Institute of Standards and Technology
NT	National Treasury
OEM	Original Equipment Manufacturer, or properly delegated legal entity representing a product brand in South Africa. Unless noted otherwise, the term includes the concepts of Brand owner and Legal entity (see Brand owner, Legal entity)
OS	Operating system
OSS	Open Source Software
PC	Personal Computer, including desktop and mobile systems
PCD	Personal Computing Device, one of the certified Technology Domains
PCI	Peripheral Component Interconnect
PFMA	Public Finance Management Act

PPPFA	Preferential Procurement Policy Framework Act
QoS	Quality of Service
RAM	Random-Access Memory
RAS	Reliability, Availability and Serviceability
RFQ/P/B	Request for Quotation/Proposal/Bid
ROE	Rate of Exchange
RSA	Republic of South Africa
SACSA	South African Communications Security Agency
SCM	Supply Chain Management
SC-ITSM	GITOC Standing Committee on IT Service Management
SITA	State Information Technology Agency
SLA	Service Level Agreement
SMME	Small, Medium and Micro Enterprise as defined and interpreted by Act 102 of 1996.
SSA	State Security Agency
SSD	Solid State Drive
TAS	Technology Advisory Services
TCO	Total Cost of Ownership: all costs associated with an ICT solution, including capital, labour, services, running costs, etc.
TCP	Technology Certification Process
TTT	Technical Task Team, a sub-committee of the GITOC SCProc.
UC	Unified Communications
USB	Universal Serial Bus
UPS	Uninterruptible Power Supply
VAT	Value Added Tax
VDI	Virtual Desktop Infrastructure
VOIP	Voice Over IP
WAN	Wide Area Network
WLAN	Wireless LAN (IEEE 802.11), also known as WiFi

Terms and Definitions

Term	Definition
Accessory	A component or subcomponent that complements or increases the capability of the offered solution. This could include software, additional parts, auxiliary products, etc.
Add-on	Component or product that complement or increase the capability of the offered product.
Base Price	The total price for all components included the Base System as specified in Paragraph A of the technical specification (Standard Components in the Excel spreadsheet).
Base system	All components included the Base System as specified in Paragraph A of the technical specification (spreadsheet).
Brand owner	The legal entity representing a product in South Africa. Legal entity status implies that the supplier is not the manufacturer of the product. The brand owner takes ultimate responsibility for branding, marketing, distribution channels and product direction. Single point of contact for Government (see Legal entity, OEM).

Term	Definition
Category	A collection of technology Items (products) representing a functional area, such as Projectors, Audio Conferencing, Recording, each containing a collection of Items. (see Item).
Channel partners	All enterprises that operate in the market as small and medium sized enterprises. An example of a channel partner is a value-added supplier that provides industry-specific software solutions and services.
Consumables	Components that have a defined life span (e.g. based on number of pages or hours used) or are consumed during the normal operation of the supplied product, including printer ink, toner, photoconductors, etc., or lamps, batteries, belts, rollers, maintenance kits, etc.
Distributor	Official channel warehousing and distribution, logistics partner appointed by the brand owner.
Component manufacturer	A third-party manufacturer of ICT components that form the basis of complete systems or solutions supplied to Government by OEMs. This includes, for example, CPU manufacturers such as AMD and Intel, drive manufacturers such as Seagate and Western Digital, or software vendors such as Microsoft, Red Hat or VMware. In this domain, some components from third-party manufacturers can be certified directly via the TCP (e.g. PCD accessories/upgrades), while others must be supplied as part of a complete solution.
Installation	Unpack system, configure, plug into power and network, integrate into venue and ensure proper operation. Installation excludes migration of software and data from previous system.
Installation charge	The price charged by the OEM’s partner to install the product in the client environment. This includes unpacking, connecting cables, power-up and user acceptance. May be required as part of the base solution price, depending on solution category or end-user requirement.
Integrator	A skilled and experienced supplier who is able to integrate the new solution into existing infrastructure or make the solution work with other solutions.
Item	Lowest-level technology subdivision in the technology domain as represented in the technical specification, e.g. VC_Soft, Proj_Basic. A product must be offered at Item level. Multiple products may be offered for each Item. Items are organised into Categories, e.g. Conferencing, Display Devices, Recording, etc. (See Category).
Legal entity	As defined by SA law, the sole OEM-appointed representative for a product brand in SA. Not necessarily the importer or distributor. (see Brand owner, OEM).
Minimum requirements	In terms of the technical specification, the lowest level of capability that will perform the required function as defined in an RFQ/RFP or client requirement. Exceeding this level is allowed, but not reaching this level will result in disqualification. (See Minimum specifications).
Minimum specifications	A specification representing a minimum technical capability. Improving on minimum spec is allowed at all times, while not complying to minimum spec will result in disqualification. For example, if 4GB storage is specified, 8GB would be accepted, but 2GB would not be. Suppliers must at all times configure offered products to meet minimum specifications (See Minimum requirements).
Model change	Replacement of an existing product by a new product due to the existing product having reached end of life, or no longer meeting requirements. A formal SITA process must be followed by OEMs to request and perform a model change.
OEM	Original Equipment Manufacturer, or properly delegated legal entity representing a product brand in South Africa.

Term	Definition
Repair	Any action taken by the OEM or service partner to ensure that a working solution is available to the client within the specified turnaround time. This can include physically repairing the system on-site, or swopping out the system or a faulty component.
Required	What the Client needs as a complete, working solution. Due to the transversal nature of the technical specification, detailed requirements cannot be addressed fully, but must be defined based on end-user requirements on a per-project basis.
Service zones	Geographical areas within South Africa where product and service delivery are required. These areas are designated as Zone A, B or C, depending on proximity to large centres. The zones are defined as follows, along with the required business-hours SLA: Zone A – **Next business day repair**: The entire Gauteng Province, as well as in or within 50km from major cities or Provincial capitals, i.e. Cape Town, Gqeberha, Buffalo City, Bisho, Bloemfontein, Durban, Mmabatho, Polokwane, Kimberley, Pietermaritzburg, Ulundi, eMalahleni and Mbombela. Zone B – **2 business day repair**: In or within 50km from major towns, i.e. Naledi (Welkom), Umtata, George, Makhanda, Thohoyandou, Madibeng, Klerksdorp, Ermelo, Standerton, Ladysmith, Oudtshoorn, Richards Bay, Saldanha, Upington, Worcester, Potchefstroom and Beaufort West. Zone C – **3 business day repair**: All towns and rural areas not included in Zone A and Zone B where services may be required. Zone C includes the entire country not covered by Zone A or B. Examples of exclusions to the on-site service requirement include equipment deployed or used on ships or other vehicles, and areas outside the immediate borders the RSA.
Supplier	Final value-added step in the channel before the end user. Compare with Solution provider
“Support for”	A capability that a product must enable, but must not necessarily have built-in or included in the base configuration without an optional accessory or upgrade.
Tech Update	Periodical refresh of technical specifications during as Government requirements change.
Technical support	A technical service rendered for out-of-warranty work, or work related to, but not covered by, the services specified as included with offered products.
Technology management	A process by which the technology specification is updated, upgraded or “refreshed” to reflect industry advancement or changes in user requirements over a period of time. The process is managed by SITA in conjunction with clients, OEMs and other role players.
Transversal Contract	A term or period contract established for more than one Government department or public body, with one or more approved suppliers for the supply of information technology goods or services over a period, required. The purpose of a transversal Contract generally can be stated as addressing 80–90% of Government requirements, reducing the need for *ad hoc* tenders. Transversal Contracts exclude niche or special requirements by definition, and there will consequently always be a need for some *ad hoc* Contracts.
Upgrades	Components or subcomponents that have the purpose of expanding the capacity of the offered product, including RAM, hard disks, CPUs, etc. Upgrades are typically expansions that can be done inside the system chassis (e.g. printer duplexer or additional RAM). “Fork-lift” replacements of systems are not seen as upgrades. Upgrades are not necessarily after-market operations. A base system may be upgraded with additional capacity at purchase time.

Term	Definition
Warranty and support	As per detail technical specifications, the following SLA conditions apply to the PCD domain: Standard warranty and support included with all supplied systems and products (as defined and qualified per technology category/Item): Countrywide on-site with full coverage (parts and labour for entire Item, upgrades and accessories) during office hours (7:30 - 17:00), with next business-day **repair** (according to Zone definitions) for 3 years (36 months) from date of delivery.
Warranty	All certified products must be warranted to be free of material and workmanship defects for the period specified in the Item technical specification. Any defects of this nature will be rectified (via repair or replacement) at the expense of the supplier under the terms specified in the Item technical specification, while maintaining minimum system availability as specified. All parts, labour and travel costs will be covered by the supplier for the extent of the warranty period. The warranty period commences from date of delivery of the product in good working order at the end-user's premises. Consumables are not covered under the warranty, except for a reasonable expectation of performance per component (e.g. batteries). Damage due to shipping is covered under the warranty. Preventative maintenance should be done by Suppliers to ensure that SLAs are maintained.