SITA

# Deployment Guidelines:
# Peripheral Devices

Version: 2.1

Date: 2024-03-15

## Notice

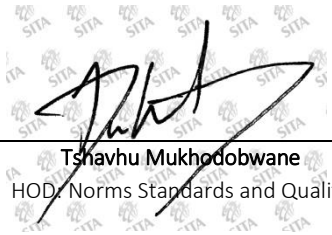


Document enquiries may be directed to:
Records Management Office
SITA SOC Ltd
PO Box 26100, Monument Park, 0105, South Africa
Tel: +27 12 482 3000
www.sita.co.za

**Deployment Guidelines: Peripheral 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.



**Tshavhu Mukhodobwane** — 27 March 2024
HOD: Norms Standards and Quality — Date

**Deon Nel** — 25/03/2024
Senior Specialist: TAS — Date

**Izak de Villiers** — 25 March 2024
Senior Specialist: TAS — Date

## Foreword

This document forms part of best practices guideline and solution selection process for Perripheral 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 peripherals, 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 **Peripherals** technology domain (including printers, multifunction devices, scanners, cameras, auto-ID and biometric devices, print management and consumables), 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 shows 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, amended periodically)
  - Engagement Model: Personal Computing Devices and Peripherals (Transversal Contract 740, amended periodically)
  - Transversal Contract RT3-2022 for the Supply, Delivery, Installation, Commissioning and Maintenance Of Office Automation Solutions
- 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: 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.

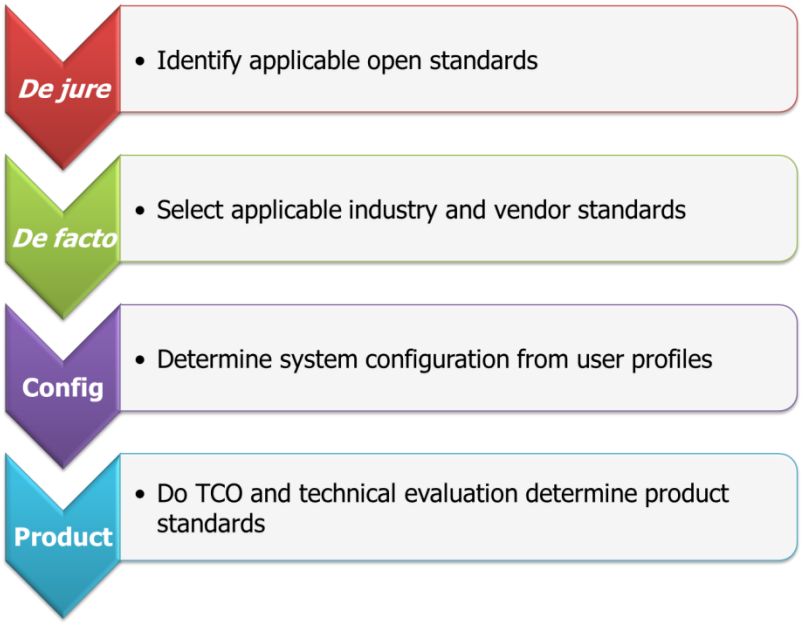



Figure 1: Standards selection process

❖ **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:

- 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.

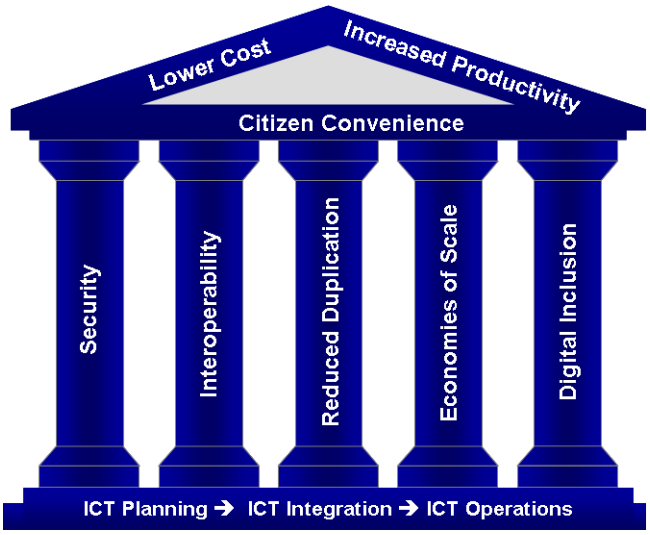



Figure 2: ICT House of Value

## 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 ICT standards, policies and Government requirements.

To support this mandate, SITA has developed, in collaboration with DPSA, GITOC and Government stakeholders, 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, and Mobile devices (Tablets, Smartphones, Industrial Handhelds). |
| **Peripherals** | **Printers, Multifunction devices, Scanners, Digital cameras, Automatic Data Capture (Barcoding, Card devices), Biometric readers, Consumables and Print management** |
| Education Solutions | Classroom solutions, including PCs, laptops, tablets, presentation and teaching devices and infrastructure hardware and software |
| Assistive Technologies | Assistive solutions (including devices and software) for people with disabilities, including smart devices (tablets, PDAs, document readers, media players, recorders and braille devices) and peripherals (input and output devices) |
| Audiovisual Communications (AVC) Technologies | Video and audio conferencing, Large-format display devices (projectors, monitors and display walls), AV cameras, Playback and recording, Collaboration, AV signal control and management, and Audio and Video components. |
| Servers & Storage | Servers (Rack-mount, Tower, Blade), Primary storage and Secondary storage (Disk to Disk, Tape and Archiving). |
| Networking | Switches, WLAN, Routers, Backhaul, Cabling (Copper and Fibre-optic). |
| Infrastructure | Equipment Racks, UPS, Generators, Cabling infrastructure, Alternative power, Cooling and ventilation |

Table 1: Certified technology domains

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.

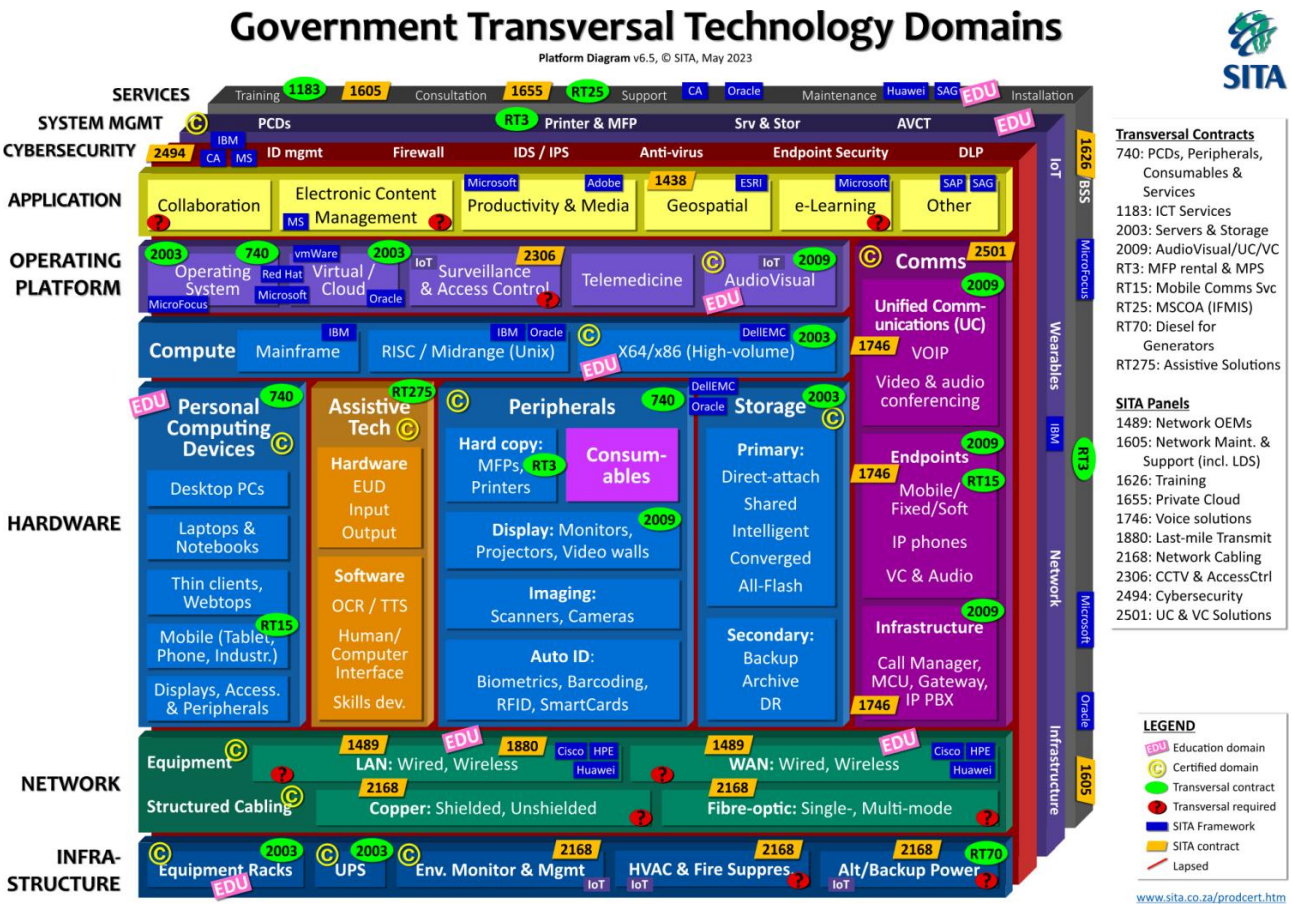



Figure 3: Certified technology domains and transversal/period contracts

The latest version of the diagram is available at [www.sita.co.za/prodcert.htm](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 Peripheral 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 Peripherals domain

The purpose of the Peripherals 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 Peripherals technology domain comprises the following categories and technology types:

| Category | Technologies |
|---|---|
| Printers | Monochrome, colour, large-format and specialised printers |
| Multifunction devices | Monochrome and Colour MFDs |
| Scanners | Document, image and large-format scanners |
| Digital cameras | Compact, system/mirrorless, DSLR and video cameras |
| Auto-ID devices | Barcode scanners and printers, ID card printers |
| Biometric devices | Signature pads and fingerprint readers |
| Consumables | Ink, toner and other consumables for printing devices |
| Device management tools | Device management tools/software for peripheral systems |

Table 2: Categories in the Peripherals 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 Peripherals 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 or 5-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 Peripherals 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 Standard printers

| Item | Description | Usage profile |
|---|---|---|
| Prn_Mono1 | Entry-level mono A4 printer | Low-volume monochrome A4 printer for single users or small workgroups, up to 5 users, or 1000 pages/month |
| Prn_Mono2 | Midrange mono A4 printer | Medium-volume monochrome A4 printer for medium workgroups, up to 15 users, or 3000 pages/month |
| Prn_Mono3 | Advanced mono A4 printer | High-volume monochrome A4 printer for large workgroups, up to 30 users, or 10000 pages/month |
| Prn_Mono4 | Midrange mono A3 printer | Medium-volume monochrome A3 printer for medium workgroups, up to 20 users, or 10000 pages/month |
| Prn_Mono5 | Advanced mono A3 printer | High-volume monochrome A3 printer for large workgroups , up to 30 users, or 20000 pages/month |
| Prn_Colour1 | Entry-level colour A4 colour printer | Low-volume colour A4 printer for single users or small workgroups, up to 5 users, or 1000 pages/month |
| Prn_Colour2 | Entry-level colour A3 colour printer | Low-volume colour A3 printer for single users or small workgroups, up to 5 users, or 1000 pages/month |
| Prn_Colour3 | Midrange colour A4 printer | Medium-volume networked A4 colour printer for medium workgroups, up to 15 users, or 3000 pages/month |
| Prn_Colour4 | Advanced colour A4 printer | Medium to high-volume networked A4 colour printer for medium workgroups, up to 30 users, or 5000 pages/month |
| Prn_Colour5 | Midrange colour A3 printer | Networked A3 colour printer for small to medium workgroups, up to 20 users, or 5000 pages/month |
| Prn_Colour6 | Advanced colour A3 printer | High-volume networked A3 colour printer for large workgroups, up to 30 users, or 10000 pages/month |

Table 3: Printer usage profiles

### 2.3.2 Specialised printers

| Item | Description | Usage profile |
|---|---|---|
| Prn_LF1 | Large format printer, A1/A2 | Large format (A1/A2) printer for line-based applications (e.g. engineering, construction and architecture) and limited high-density printing (e.g. maps, media and rendering) |
| Prn_LF2 | Entry-level large format printer, A0 | Entry-level large format (A0) printer for line-based applications (e.g. engineering, construction and architecture) and limited high-density printing (e.g. maps, media and rendering) |
| Prn_LF3 | Advanced large format printer, A0 | Advanced large format (A0) printer for line-based applications (e.g. engineering, construction and architecture) and limited high-density printing (e.g. maps, media and rendering) |
| Prn_Port1 | Portable printer | Portable, battery-powered printer for mobile colour printing |
| Prn_Impact1 | Slip/POS printer | Slip printer for service desk and point-of-service applications (e.g. pharmacies) |
| Prn_Impact2 | Entry-level impact printer | Entry-level 80-column impact printer for low-volume report printing, multipart stationery, and mainframe printing. (up to 2 users) |

| Item | Description | Usage profile |
|---|---|---|
| Prn_Impact3 | Advanced impact printer | Advanced 136-column impact printer for medium-volume report printing, high-impact multipart stationery, and mainframe printing (up to 5 users) |

Table 4: Specialised printer usage profiles

### 2.3.3 Multifunction devices

| Item | Description | Usage profile |
|---|---|---|
| MF1 | Entry-level A4 mono MFP | Low-volume monochrome A4 multifunction printer for low-volume desktop or workgroup printing, copying and scanning, up to 5 users, or 2500 pages/month |
| MF2 | Midrange A4 mono MFP | Medium-volume monochrome A4 multifunction printer for workgroup printing, copying and scanning, up to 15 users, or 5000 pages/month |
| MF3 | Advanced A4 mono MFP | High-volume monochrome A4 multifunction printer for workgroup printing, copying and scanning, up to 30 users, or 10000 pages/month |
| MF4 | Midrange A3 mono MFP | Midrange monochrome A3 multifunction device for high-volume workgroup printing, copying and scanning, up to 30 users, or 15000 pages/month |
| MF5 | Advanced A3 mono MFP | Advanced monochrome A3 multifunction device for high-volume workgroup printing, copying and scanning, up to 50 users, or 30000 pages/month |
| MF6 | High-end A3 mono MFP | High-end monochrome A3 multifunction device for high-volume workgroup printing, copying and scanning, 50+ users, or 60000 pages/month |
| MF_Prod | Mono production printer | Production-level colour monochrome A3 printer for high-volume enterprise printing, 150000 pages/month |
| MFC1 | Entry-level A4 colour MFP | Low-volume colour A4 or A3 multifunction printer for low-volume desktop or workgroup printing, copying and scanning, up to 5 users, or 1000 pages/month |
| MFC2 | Midrange A4 colour MFP | Medium-volume colour A4 or A3 multifunction printer for workgroup printing, copying and scanning, up to 15 users, or 2500 pages/month |
| MFC3 | Advanced A4 colour MFP | High-volume colour A4 or A3 multifunction printer for workgroup printing, copying and scanning, up to 30 users, or 7500 pages/month |
| MFC4 | Midrange A3 colour MFP | Midrange colour A3 multifunction device for high-volume workgroup printing, copying and scanning, up to 30 users, or 15000 pages/month |
| MFC5 | Advanced A3 colour MFP | Advanced colour A3 multifunction device for high-volume workgroup printing, copying and scanning, up to 50 users, or 20000 pages/month |
| MFC6 | High-end A3 colour MFP | High-end colour A3 multifunction device for high-volume workgroup printing, copying and scanning, 50+ users, or 30000 pages/month |
| MFC_Prod | Colour production printer | Production-level colour A3 printer for high-volume enterprise printing, 80000 pages/month |

Table 5: Multifunction device usage profiles

### 2.3.4 Scanners

| Item | Description | Usage profile |
|---|---|---|
| Scan_Doc1 | Desktop document scanner | Desktop A4 document scanner |
| Scan_Doc2 | Entry-level document scanner | Low-volume A4 document scanner |
| Scan_Doc3 | Midrange document scanner | Medium-volume A4 document scanner |
| Scan_Doc4 | Advanced document scanner | High-volume A3 document scanner |
| Scan_Doc_Prod | Production document scanner | Production-level A3 document scanner |
| Scan_Doc_Net | Network document scanner | Low- to medium-volume network-attached scanner for shared workgroup on-demand scanning |
| Scan_Doc_Port | Portable document scanner | Portable, low-volume USB- or battery-powered document scanner |
| Scan_Img | Desktop A3 image scanner | A3-size flatbed desktop image scanner for document capture, as well as graphics and design applications |
| Scan_LF1 | Basic large-format image scanner | Entry-level large-format scanner (A0 / A1 / A2) for engineering, mapping and imaging applications |
| Scan_LF2 | Advanced large-format image scanner | Advanced large-format scanner (A0 / A1 / A2) with enhanced image quality for engineering, mapping, imaging and artwork applications |

Table 6: Scanner usage profiles

### 2.3.5 Auto-ID devices

| Item | Description | Usage profile |
|---|---|---|
| Scan_BC1 | Barcode scanner | Corded barcode scanner with support for linear and/or 2D barcodes |
| Scan_BC2 | Cordless barcode scanner | Cordless barcode scanner with support for linear and/or 2D barcodes |
| Prn_BC1 | Portable barcode/ label printer | Portable, battery-powered barcode and label/slip printer |
| Prn_BC2 | Desktop barcode/label/POS printer | Office barcode and label/slip printer for point-of-service and general applications |
| Prn_BC3 | Advanced barcode/label/POS printer | Advanced barcode and label/slip printer for more demanding point-of-service and specialised applications |
| Prn_Card1 | ID card printer | Entry-level card printer with support for multiple auto ID technologies for basic, low-volume ID card production |
| Prn_Card2 | Advanced ID card printer | Advanced card printer with support for multiple auto ID technologies for medium-volume ID card production |

Table 7: Auto-ID usage profiles

### 2.3.6 Biometric devices

| Item | Description | Usage profile |
|---|---|---|
| SigPad1 | Basic signature pad | Entry-level signature pad for e-signature applications with monochrome display, support for biometrics |
| SigPad2 | Midrange signature pad | Midrange signature pad for e-signature applications with monochrome display, and support for biometrics |
| SigPad3 | Advanced signature pad | Advanced signature pad for e-signature applications with programmable colour display, support for biometrics and encryption |
| Biometric1 | Biometric reader, single fingerprint | Single-finger fingerprint biometric reader for logical access control, user authentication and biometric enrollment |
| Biometric2 | Biometric reader, multi-fingerprint | Multi-finger or palmprint biometric reader for identification and/or biometric enrollment |
| Biometric3 | Biometric reader, contactless modalities | Contactless desktop biometric reader (e.g. face, iris or palm modalities) for logical access control, user authentication and biometric enrollment |

Table 8: Biometric usage profiles

### 2.3.7 Digital cameras

| Item | Description | Usage profile |
|---|---|---|
| Cam_Compact | Advanced compact digital camera | Advanced compact digital camera with high-end exposure controls for media, office and business photography |
| Cam_CSC | Compact mirrorless camera | Digital compact system camera (CSC) with mirrorless design, interchangeable lenses and advanced exposure controls |
| Cam_Sys1 | Basic system camera | Basic digital system camera (mirrorless/DSLR) with interchangeable lenses and advanced exposure controls |
| Cam_Sys2 | Advanced system camera | Advanced digital system camera (mirrorless/DSLR) with interchangeable lenses, advanced exposure controls and high-performance image processing capabilities |
| Cam_Vid1 | Professional digital video camera | Digital video camera for business use, including teaching/training, communications, media and office use |
| Cam_Vid2 | Advanced digital video camera | Advanced digital video camera with manual controls and high-end video capturing and processing capabilities |

Table 9: Digital camera usage profiles

### 2.3.8 Consumables and Device Management

| Item | Description | Usage profile |
|---|---|---|
| Consum | Consumables for printing devices | Range of alternative or third-party consumables for printing devices currently and previously certified by SITA and in use by Government. Includes toner cartridges, drums, ink, printheads and other printer consumable components |
| Mgmt | Print management | Print management tools/systems, offering device and/or user management to enable cost reduction or value-added services for printing systems. Including e.g. reporting, alerts, tracking, deployment support and access control |

Table 10: Consumables and Device Management usage profiles

## 2.4 Bundled accessories and support

Each Peripheral Item is specified as a **fully working solution** with a minimum set of mandatory bundled consumables, accessories and services. For example, all printing devices are bundled with a mandatory SLA, full set of consumables, drivers and all required cables. None of these components may be left out by suppliers, but Government may substitute the default components with alternatives or upgrades (e.g. higher-yield consumables or additional paper trays). Departments do not need to specify any components or configurations to get a working system, unless there are additional requirements (e.g. a card reader or upgrades to the standard support SLA).

The specification prevents suppliers from quoting or delivering incomplete solutions (e.g. printers without consumables or paper trays, or cameras without lenses), and suppliers are mandated to quote and deliver fully working solutions.

Mandatory support SLA: all devices in the Peripherals 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.

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. Peripherals 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. exact weights and measurements) must **not** be used to define an end-user requirement. The **business need** must be defined based on actual usage requirements.
- The Peripherals domain focuses 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 Peripherals, is that the **end-user requirement** must determine the type of system or device that must be procured. In the Peripherals 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 label printer for inventory management).

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.

## 3.3 Printers

In terms of printing devices, Departments must first carefully consider whether a document absolutely needs to be printed, in order to contain operational costs as far as possible. Once that has been determined, a cost study must determine the most appropriate printing device.

To decide on a printer for an end-user requirement, several questions need to be answered to analyse printing needs:

- **Is a hard copy really necessary?** The first question is whether a document actually needs to be printed, or whether it can be processed and distributed electronically. Departments must be aware of the costs and impact of printing large volumes of paper. Cost studies can help highlight these costs, and also identify alternatives such as ECM (electronic content management). In the case of very large print runs, Departments should consider using in-house bulk printing instead of standard office printers, or to outsource these jobs to SITA's specialised high-volume printing and document delivery service.
- **Colour or monochrome:** Is there a requirement for colour printing (typically more expensive to buy and operate), or is black-and-white sufficient?
- **Page size:** Size of documents that need to be printed? Choices include A4, A3 or larger (up to A0), and can include multiple sizes in a specific requirement (e.g. A0, A1 or A2 maps, A4 or A3 documents or reports).
- **Print volumes:** What number of pages needs to be printed on a daily or monthly basis? Actual paper usage, as well as the volumes printed by existing devices should be used as input into this figure to increase accuracy. Volumes must be broken down per paper type/size and per colour/monochrome.

- **Number of users:** How many users will be using the device on a daily basis? This often relates directly to the print volume requirement, but also factors into the accessibility of the device.
- **Connectivity, host system and applications:** Which types of networks, systems and applications will be producing output for the device? Compatibility and application-specific needs must be considered. Example of host systems or connectivity could be the mainframe, USB, Bluetooth or direct LAN attachment, or legacy connectivity such as Parallel or Serial.
- **Specialised print requirements:** Portable printing, impact printing, slip printing, barcode printing and large format are all addressed via the Peripherals domain.
- **Physical location:** Will the device be deployed on a desktop, or as a floor-standing system? This determines whether a printer stand or trolley is required. All peripherals, doors, trays, etc. must be easily accessible by users and technicians.

The diagram below illustrates the various types of printing requirements, and how they translate to a specific class or type of printing solution. Once the type of solution has been identified, the **detail business requirements** must be specified to ensure the proper device is selected.

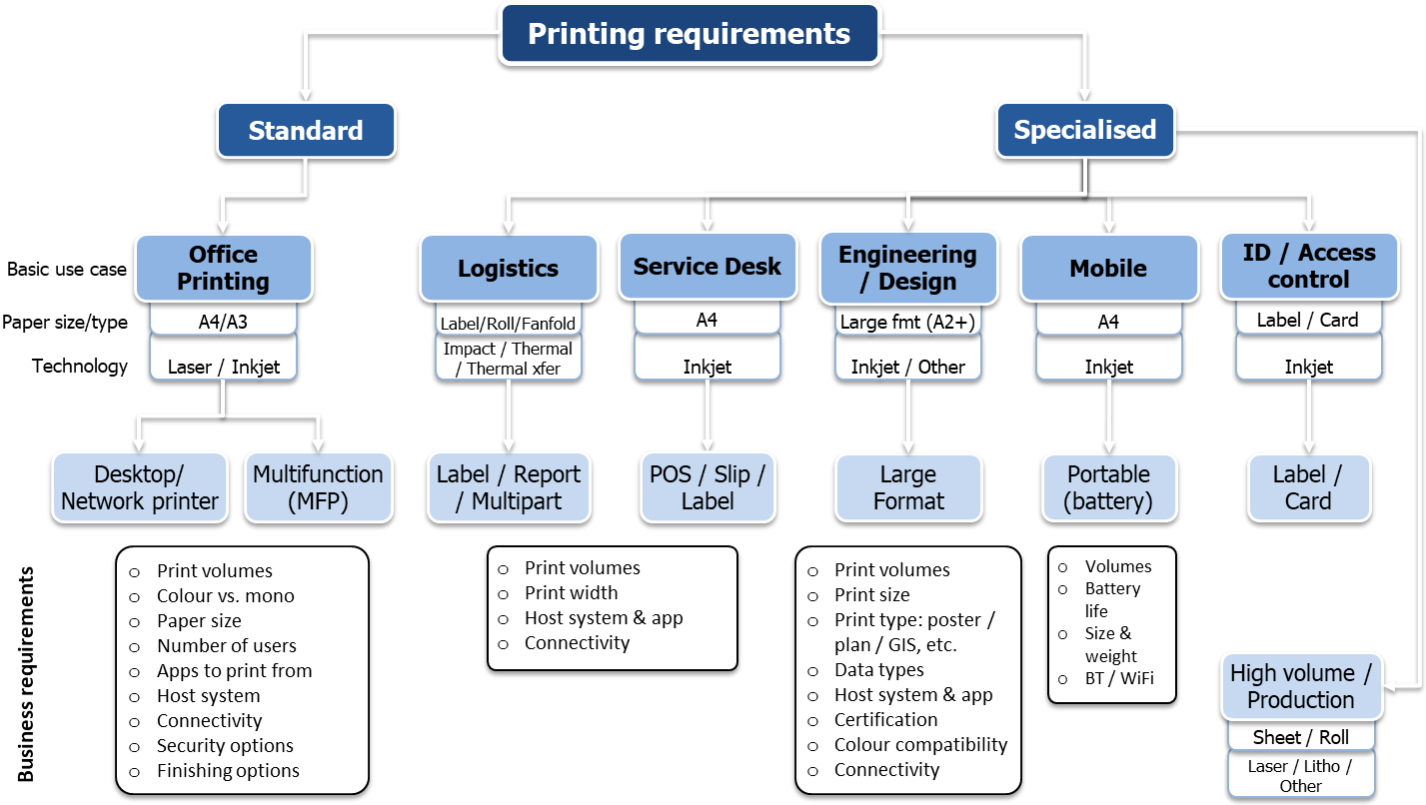



Figure 4: Business requirements, selection guidelines and usage models for printing devices

### 3.3.1 Print volumes

Print volumes are one of the most important criteria in selecting a printing device. Volumes can be roughly divided into the following size categories, which are typically significantly different for monochrome and colour printing.

| Volume description | Typical number of pages | |
|---|---|---|
| | Daily | Monthly |
| Low | <50 | <1 000 |
| Medium | 150 – 250 | 3 000 – 5 000 |

| Volume description | Typical number of pages | |
|---|---|---|
| | Daily | Monthly |
| High | 500 – 1 000 | 10 000 – 20 000 |

Table 11: Print volume categories (monochrome)

| Volume description | Typical number of pages | |
|---|---|---|
| | Daily | Monthly |
| Low | <25 | <500 |
| Medium | 50 – 150 | 1 000 – 3 000 |
| High | 250 – 500 | 5 000 – 10 000 |

Table 12: Print volume categories (colour)

The same volume categories can be applied for multifunction devices, with the major difference being that printers are single-function, while MFD devices offer scanning, faxing and copying in addition to printing, which significantly affect the day-to-day volumes. Information on MFD capabilities and user/volume values can be found in the detail specifications.

### 3.3.2 Running costs (TCO)

One of the most important factors in purchasing a printing device is the cost to operate it over time. For example, the consumables required for colour printers can cost many times their purchase price over the lifetime of the device. When factoring in consumables and energy use, a standard office laser printer can often cost **10 times** its purchase price over its lifespan. Departments must carefully calculate the page volumes the device will be printing over its life before selecting a printing technology and device.

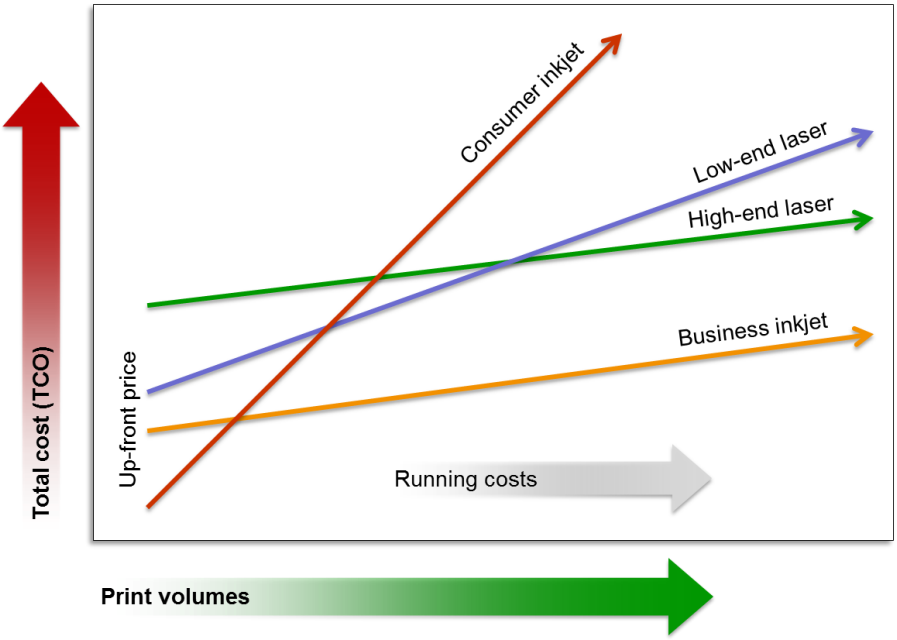



Figure 5: Total cost per printing technology type

The diagram below illustrates the costs associated with printers, with the start of each line representing the acquisition cost, and the angle of the line representing the running costs over time. It is clear that certain technologies (e.g. consumer inkjets) are very cheap to buy, but very expensive to run over time. In general, higher-end devices have higher purchase prices, but lower running costs. For a given volume, therefore, Departments must calculate the break-even point for each technology to identify the appropriate solution. TAS is available to help with cost calculations if required.

The table below is a cost calculation comparing two inkjet printers, with the low-end one being a typical home-focussed, "cheap" printer, and the other a high-duty cycle business-focussed device. Note that the "expensive" device is almost **3 times cheaper** to run over time.

| | Retail | Enterprise |
|---|---|---|
| |  |  |
| **Price** | R380 | R1330 |
| **Ink prices** | Black: R 145<br>Colour: R 170 | Black: R 295<br>Colour: R 195 |
| **Ink yield (pages)** | Black: 200<br>Colour: 165 | Black: 2200<br>Colour: 1400 |
| **Duty cycle per month** | 750 pages | 15000 pages |
| **Print speed** | 16 pg/min | 34 pg/min |
| **Ink cartridges** | 2: K + Tricolour | 4: CMYK |
| **Cost per page** | R1.76 | R0.55 |
| **Pages per month** | 200 | 200 |
| **TCO over 3 years** | **R 8 810** | **R 3 980** |
| **TCO over 5 years** | **R 17 240** | **R 6 630** |

Table 13: Difference in TCO between "cheap" and "expensive" printers

### 3.3.3 Additional printing guidelines

- According to industry sources, producing a piece of paper can take up to 20 times more energy than printing on it, and therefore effective use of paper (e.g. less printing, duplex, n-up) can have a significant impact on the environment.
- Given the environmental impact of printing in general (paper and energy use, amongst others), printing should be restricted where possible. According to Gartner, 22% of printed documents are never used, 34% are used for less than 5 minutes, and 50% of prints are discarded within a day.
- Deploy **appropriate drivers and settings** for end-user requirements: no unnecessary functions should be available to users. This can lighten the ICT management burden in Departments and lower printing costs.
  - Configure drivers with duplex and toner save mode as default. Settings such as Booklet can be used to save paper by making end-users aware of them.
  - Colour printers should be configured to print monochrome by default, with authorised users being allowed to select colour printing on demand.
  - Some OEMs offer lighter "enterprise" versions of their drivers, as well as universal drivers which support a wide range of printers. Since this reduces complexity and increases commonality, Departments are encouraged to make use of these options.
- In general, colour printing is still expensive; Departments should control colour printing facilities carefully to keep costs low. Colour printing should be made available only to users who specifically need the function.
- **Brand- and model-specific consumables**: Given that consumables (e.g. ink or toner) are <u>always</u> procured for a specific product deployed in Government, RFQs sourcing these consumables <u>must be model-specific</u>. Suppliers must know which product the consumables are for to quote accurately, and Government must be sure that the sourced consumables will work in their printer to avoid fruitless expenditure.
- **Alternative or third-party consumables**: Departments are allowed to purchase alternative (non-OEM) consumables. However, refilled or other poor-quality (non-certified) consumables are not allowed

due to quality and cost issues. Departments should take great care when selecting alternative consumables, since damage to printers due to these consumables will void the warranty. **Only** consumables that have been **certified by SITA** should be purchased. This topic is discussed in greater detail in **Section 3.8**.

- Instead of buying pre-printed forms, use the **print-on-demand** function available on many printers to reduce paper wastage and external printing costs.
- Note that many printing devices are shipped with "**starter cartridges**" with significantly lower page yield. Ensure that a full additional set of consumables is included when ordering the printer to ensure business continuity and lower long-term cost.
- **Large format printing**: Several factors need to be taken into account when selecting a large format printer, including the type of printing to be done (lines, text, maps, posters, photos, renders); print volumes and typical job length (impacting paper roll size and number); paper types (bond, photo, film, matte, gloss); durability of print and expected life (e.g. indoor/outdoor use); and multifunction requirements (print/scan/copy).
- **Best practice for WiFi**: To ensure a more secure and reliable connection, printers and MFPs should be wired where possible. WiFi should only be used where cabling is impractical, and must be deployed according to best practices in terms of security, coverage and performance.
- **Efficient use of printing systems**: Energy saving must be enabled on printing devices to allow Sleep Mode for low-usage periods, which can be used in conjunction with scheduled wake-up times on weekdays. Printing must be double-sided where possible, and features such as booklet or n-up printing must be enabled for users. Colour printing should only be used when absolutely necessary.
- **System management security**: Information gathering from printing devices should be done via e-mail (SMTP), not allowing service providers to connect directly to Government devices.
- **Power supply reliability**: To avoid wastage of ink and possible damage to print heads or other sensitive mechanisms, large format scanners and printers should be connected to a UPS.
- **Load shedding**: in order to mitigate productivity issues due to load shedding, Departments are encouraged to deploy printing devices with lower power consumption, such as inkjet devices that use significantly less electricity, and can typically be run from UPS power.

## 3.4 Multifunction devices (MFPs)

**Responsibility within the organisation:** Traditionally, MFPs ("copiers") have been procured and managed by the Office Services group within Departments, not by IT. However, since the convergence of ICT and Office Automation happened, office copiers are clearly ICT, and not office automation products. According to the SITA Act, if the **primary** function of a product is to process and communicate information, it is ICT. Given the fact that that MFPs are complete Unix/Linux computers connected to the LAN, often connected to the internet with access to the entire enterprise network. This implies that MFPs have to be configured and managed as ICT devices, since all ICT security and manageability risks apply to MFPs.

In addition to all the considerations for printers, the following additional factors apply to MFPs:

- **Document management requirements:** In the case of an MFP, will it need to process significant volumes of documents from a scanning and ECM perspective? If scanning is a significant part of the requirement, the criteria for document scanners below must be incorporated into the proposal.
- **Peripherals and finishing options:** Which types of attachments or accessories are required for the printer? This may include biometrics, card readers, finishers, staplers, additional paper trays, etc. This becomes an important productivity issue in high-volume or production environments.
- **Analogue fax:** For all practical purposes, fax has disappeared as a requirement with Government, although some Departments still order fax-capable devices. Note that this must be specified as an

additional requirement, since most devices do not have fax configured as default. Departments should investigate migrating away from analogue fax to a digital solution, which could include a centralised fax server, or fax to e-mail system.

## 3.5 Scanners

The Scanner category is divided into **document** scanners and **image** scanners.

The primary selection criterion for document scanners is **scan volume** (i.e. the number of pages to be scanned per project or over a time period), after which paper types and sizes or additional accessories such as endorsers come into play. Typical scan volumes can be roughly divided into the following size categories:

| Volume description | Typical number of pages | |
|---|---|---|
| | Daily | Monthly |
| Low | 200 | 4 000 |
| Medium | 5 000 | 100 000 |
| High | 10 000 | 200 000 |
| Production | 50 000 | 1 000 000 |

Table 14: Scan volume categories

### 3.5.1 Document scanning

The following criteria must be used to determine which document scanner or scanning solution to procure:

- Scan volumes (pages per day/month) – minimum and maximum + worst-case peaks
- Document/paper types, content and quality:
  - Paper size (A8 – A0): break down the sizes per volume
  - Paper sizes and types (fragile, thick, small)
  - Paper thickness: very thin (~50gsm) or thick board?
  - Highlights, noise, light/faint text, dot matrix
  - Document backgrounds (e.g. coloured paper)
  - Colour content vs. black & white
  - Double-sided/single-sided (simplex/duplex scanning)
  - Single-page or multi-page documents
  - Fragile, crumpled or torn
  - Folded or bound (stapled, punched, etc.)
  - Very thick or large documents (possible requirement for flatbed scanning)
  - Documents already sorted in types, or will document batches be mixed
- Existing scanners and scanning processes (if any)
- Existing or new ECM solution (integration vs. new development)
- Accessibility of the documents
- Infrastructure and other resources:
  - For on-site processing, is there sufficient dedicated physical space for a back-scanning project?

- Resources, processes and space for preparing documents
- Data storage, process and system for indexing and storing, post-scanning
- Hours available for scanning, including Limited limitations times for scanning (e.g. just mornings)
- Operator/user skills and training

- Scanner output:
  - Scan resolution: 300dpi is recommended as a minimum, since it results in higher-quality images, and allows more effective OCR.
  - Colour vs. monochrome
  - File formats, e.g. TIFF, PDF
  - Connectivity type: network, local (USB)
  - Scanner software interface (TWAIN/ISIS)
- Document analysis such as barcode scanning, or OCR/ICR.
- Processing steps such as imprinting/endorsing or patch codes
- Maximum size of batches (document feeder size)
- Centralised vs. distributed scanning
- On-demand, day-to-day vs. back-scanning
- On-site vs. off-site scanning (security and logistics implications)
- Transport and archiving of scanned and processed data
- Complementary services required:
  - Document sorting
  - Document preparation
  - Indexing
  - Quality Assurance / proofing
  - OCR
- Indexing:
  - Fields for database
  - Automatic vs. manual

## Other recommendations

- Keep a set of consumables ready to avoid delays in the scanning process.
- Ensure the scanner is used within its recommended operating parameters, and not being run beyond its rated volume – this will void the manufacturer warranty in case an issue arises.
- Scanner must maintained as per manufacturer instructions. This includes regular cleaning, cleaning/replacement of rollers, etc.
- To avoid delays or performance issues, the configuration of the scanning station for high-speed/large-format scanners should be adequate for the large data volumes. For example, a single A0 300-dpi colour page requires more than 400MB of raw data to be transferred from the scanner to the PC. As can be seen from the table, colour images (even when compressed with a lossy algorithm) take up 9–10X more storage space than monochrome images. Lossless images can take up to 25X more storage space than lossy ones, which would be unrealistic to store in any high-volume scenario.

| Paper size | Compressed image size @ 300 dpi | |
|---|---|---|
| | Mono (lossless) | Colour (lossy) |
| A4 | 110KB | 1.1MB |
| A3 | 210KB | 2.1MB |
| A0 | 1.8MB | 16MB |

Table 15: Storage space per image/page type

- To minimise throughput bottlenecks in the document capture process, ensure that the following are adequately addressed:
  - Performance of scanning station: system must have adequate connectivity, storage, RAM and processing power to handle the maximum document output from the scanner.
  - Speed and efficiency of scanner operators, QA and indexing workers: people are often the most difficult bottleneck to manage: ensure that operators are adequately trained, and are proficient with the scanning and indexing systems and equipment.
  - Document preparation is a major bottleneck: a lot of work needs to be done up-front to make sure paper is ready to be scanned. This includes removing it from files, removing staples and paper-clips, stacking and sorting (if necessary). In most cases the amount of time taken to prepare the documents is several times more than what the scanner takes to ingest and output the pages.
  - Quality assurance is a major factor in ensuring that the scanning process is successful. If the scanner output is not checked against pre-defined quality parameters, the scans may be unusable. This must be picked up early in the process in order to rectify any issues and recapture the sub-standard scans.

## 3.6 Digital cameras

Digital cameras are divided into **still** and **video** cameras, with further choices between capabilities and advanced functionality depending on requirements. The point-and-shoot camera is reasonably easy to use and cheaper to purchase, while system-based models such as DSLR and mirrorless allow users to purchase additional lenses and other accessories for specific requirements.

Most digital cameras offer optical image stabilisation to enhance image quality for hand-held operation. For certain use cases (e.g. low-light photography without flash), this can have a significant impact on performance, and users are encouraged to specify this technology where appropriate.

New technologies such as AI-based image enhancements must be used with caution in order not to distort the factual accuracy of captured images.

Criteria for camera selection:

- Still vs. video
- Subject matter
- Typical use case
- Typical lighting conditions (e.g. indoors/outdoors, day/night)
- Image resolution and quality
- Accessories required: lenses, tripod, carry bag, storage

## 3.7 Auto-ID devices and solutions

When specifying labelling and scanning solutions, the following factors must be taken into account:

- System integration requirements: what needs to be done to integrate the device into the system
- Requirement for bespoke development: SDKs must be made available as part of the solution
- Physical environment (office, store, outside, dust, heat, dirt, chemicals, etc.)
- Lighting (e.g. direct sunlight, electrical lights, darkness)
- Connectivity: physical to host (e.g. USB, Bluetooth) and logical to back-end systems
- What the device will connect to (host PC, tablet, etc.)
- Mobility: device weight and size, screen size, battery life
- Application(s) to run on device (if any)
- User interface for handheld devices
- Type of barcodes to be read (it is recommended that the actual codes be tested on prospective scanners to ensure interoperability before procurement)
- How the capturing process will work

## 3.8 Consumables

Consumables are certified and listed part of the certified OEM printer, not as individual components. Once an OEM product is certified, the related OEM consumables are also certified for the life of the device, to ensure that Government can continue operating the device for its entire useful lifecycle.

### Third-party consumables

In the case of **third-party** (non-OEM) consumables, Departments must check that the relative cost of the consumable is lower than the corresponding OEM product. Note that only **SITA-certified** consumables may be purchased. Any issues with quality or service delivery must be reported to SITA for action.

SITA's specification/standard for consumables was established in 2012 via the standard GITO Council process. Government and industry collaborated in the development of the specification, which was ratified via the proper GITOC channels.

The background to the development of this standard is that Government often purchases poor-quality **refilled** cartridges, which are very cheap, but cause problems with **reliability** and **print quality**. Government requested SITA to develop a standard by which **lower-cost consumables** can be procured, since OEM consumables were deemed too expensive.

As part of the product certification process, SITA examines the product manufacturing process and physically tests representative samples for quality and compatibility in our Lab. Products that do not meet the standard are **not** certified. Products that meet all the requirements are **certified by SITA** in accordance with National Treasury mandates. Any product that does not have a SITA certificate should **not** be procured.

The SITA Consumables standard is very strict, requiring at least the following from submitted products:

- Manufacturing processes: ISO-certified manufacturing and environmental certification (ISO9001 and ISO14001).
- Equivalent print quality as that delivered by OEM consumables.

- Same or better ink/toner yield as OEM (number of pages per cartridge). This translates to the same or better cost per page as the OEM product.
- Industry-standard yield and quality testing.
- At least 2 years on-site warranty and SLA on consumable products.
- Printer is warranted by the consumable OEM – a guarantee is required from the consumable supplier: if the consumable damages the client's printer, the printer must be repaired at the cost of the consumable OEM.

The full SITA Consumables specification can be accessed at www.sita.co.za/prodcert.htm, as part of the Peripherals Detail Spec.

From SITA's perspective, all of the risks regarding running cost, reliability and quality have been addressed, and therefore we encourage Government to seriously consider purchasing SITA-certified 3rd-party consumables, as they contribute to lowering TCO without increasing risk.

Note: Departments must ensure that delivered consumables are **actually** SITA-certified – packaging must be properly branded, not generic white boxes, and the markings on product itself must correspond to the SITA certificate.

## 3.9 Device management tools

These tools or systems can enable Departments to contain costs by allowing accurate tracking, control and costing of ICT systems. This category includes asset tracking and security tools, and printer fleet management. A wide variety of devices is supported, and Departments must stipulate exactly which products must be managed as part of the request. Costing must be carefully examined to ensure a cost-effective deployment that will save operational costs without increasing capital/licencing expenses disproportionately.

As with other software licencing, it is recommended that Departments procure licences to cover the entire warranty/SLA period for the devices to be managed. Periodic payments typically increase administration and inefficiencies compared to a single up-front payment.

## 3.10 Biometrics

As noted above, biometrics provide access control systems the ability to move beyond token- or PIN-based identification to more permanent and non-repudiable metrics by measuring and quantifying certain physical characteristics of the user, such as:

- Fingerprints
- Face
- Hand geometry
- Iris and retina
- Vein patterns in the palm or finger
- Behavioural metrics such as keystroke, signature or gait analysis.

Among biometric modalities fingerprint is by far the most-used and most mature and well-understood. However, the need to remove physical contact during COVID has prompted consideration of alternative, touchless metrics such as face.

The complexity of biometric systems and technologies require special care during system design and implementation in order to ensure a successful access control solution. For example, there are rare

individuals whose biometrics (whatever type) cannot be accurately captured or measured, and hence they can either not be enrolled in the system, or they cannot be verified by the system. Provision must be made for such users by allowing alternatives such as tokens, passwords or even dual-mode readers (e.g. finger and face).

A comparison of the main biometric modalities is provided in the table below, along with ratings for various metrics pertaining to the relative value of each modality. Departments can use this information to choose the most appropriate biometric, given the inevitable trade-offs: for example, a more secure modality typically results in a more expensive access control system, while a cheaper reader is typically less secure and trustworthy.

| Biometric | Availability | Uniqueness | Permanence | Acceptability | Attack risk | Relative cost |
|---|---|---|---|---|---|---|
| Fingerprint |  |  |  |  |  |  |
| Face |  |  |  |  |  |  |
| Hand geometry |  |  |  |  |  |  |
| Iris |  |  |  |  |  |  |
| Retina |  |  |  |  |  |  |
| Keystroke |  |  |  |  |  |  |
| Voice |  |  |  |  |  |  |
| Palm vein |  |  |  |  |  |  |
| Finger vein |  |  |  |  |  |  |

Table 16: Comparison of biometric modalities

| Definitions | |
|---|---|
| **Availability** | Likelihood that users will consistently be able to accurately present the biometric for enrolment |
| **Uniqueness** | Likelihood that the selected biometric is not repeatable across a population |
| **Permanence** | Likelihood that the selected biometric will remain stable over time and resist conditions that make it unavailable |
| **Acceptability** | Likelihood that users will accept and use the biometric |

## Degrees of correctness

An important property of biometrics in general is that the output is not "digital", as is the case for most other IT concepts: we are accustomed to systems with a hard "Yes or No", or "1 or 0". If a user enters his password correctly, the result is clear, as it would be in the opposite case: the system knows whether to allow or deny access. In the case of biometrics, the result is always on a spectrum of probability, not a 1 or 0. This means that the system or reader must be tuned to attain the desired level of security, which must be balanced against the level of "friendliness" to users. Hence the concepts of FRR and FAR:

| | |
|---|---|
| **FRR** | False Reject Rate: likelihood that an authorised user is denied access |
| **FAR** | False Accept Rate: likelihood that an unauthorised user is granted access. |

These two concepts are directly related to the security and user-friendliness of the system, in an inverse relationship. This means that the more secure the biometric's FRR/FAR tuning (e.g. choosing a lower FAR), the more likely the system is to reject legitimate users, making it more "unfriendly". Conversely, the more "friendly" the tuning becomes (i.e. choosing a lower FRR), the less secure the system. The graphic illustrates the relationship between these two rates.

In short, in order to avoid customer backlash, an organisation such as a bank would rather allow a few unauthorised users access rather than lock out legitimate customers. The bank would therefore choose a lower FRR, allowing a higher FAR.

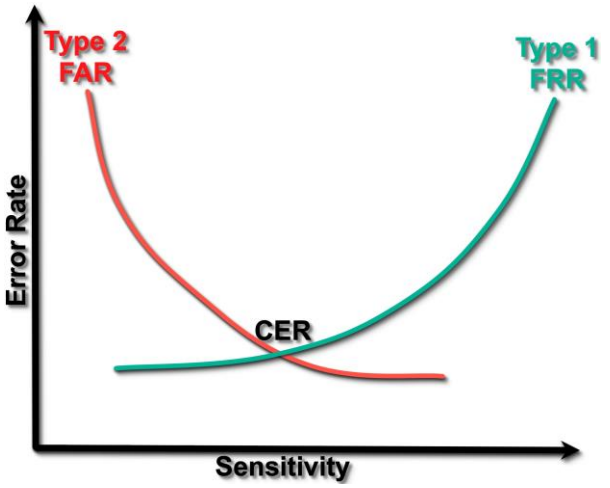



Figure 6: Biometric FRR vs. FAR

On the other hand, a Defence installation has no customers, but places a very high emphasis on security. Denying access to a few legitimate users is more acceptable in this scenario, hence the facility would choose a lower FAR, accepting the inevitable rise in FRR and a few angry users.

## Enrolment and verification

As noted above, enrolment is a vital step in biometric access control: if this is done improperly, the system cannot hope to be successful.

The enrolment process typically requires a PC-connected enrolment reader, deployed in an ideal environment (e.g. correct lighting conditions for face recognition, controlled moisture levels for fingerprint, etc.) This installation must match the specified biometric requirements of the chosen readers (templates, accuracy, etc.). A detailed procedure must be developed, operators must be properly trained and they must not deviate from the procedure for all enrolments.

The image below illustrates the process of enrolling a new user into the biometric access control system. In short, the biometric is captured by the reader, converted into a biometric template by extracting the relevant features, and then stored in an access control database (AD in this case.

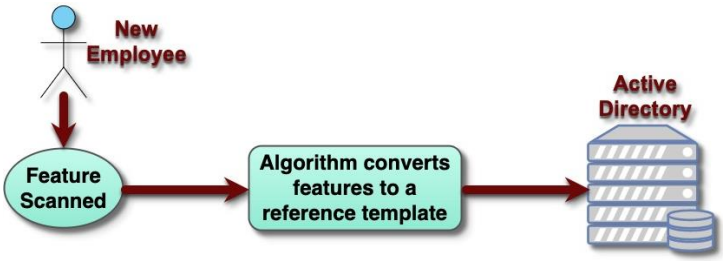



Figure 7: Biometric enrolment

When the user wants access to the facility, they present their credentials and their biometric (fingerprint, face, etc.), at which time the reader captures the biometric, converts to template and this gets matched with the template in the database. In case of a match, the user's identity is deemed to be verified, and access is granted.

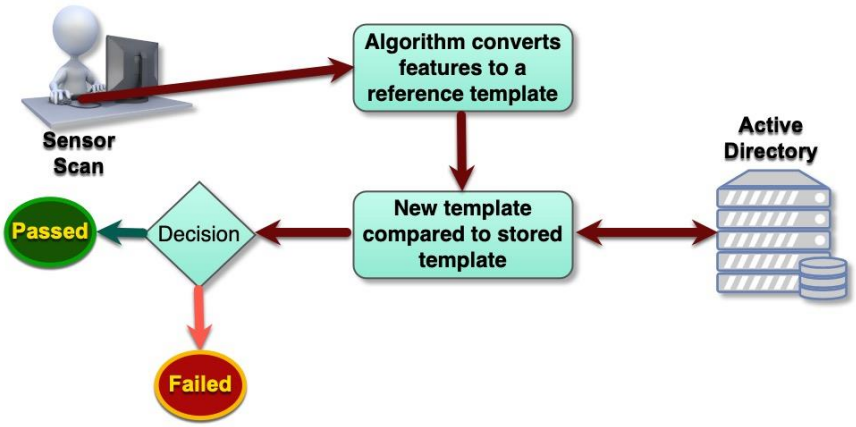



Figure 8: Biometric verification (pass/fail)

### 3.11 Secure configuration of systems

The following security recommendations apply to multifunction devices, printers and other network-attached peripherals:

- Enable user authentication or access control
- Set a strong administrator password
- Disable unused ports and systems (e.g. FTP, POP3)
- Set passwords for user mailboxes
- Disable USB ports if they are not used or needed in the environment
- Enable hard drive encryption
- Securely erase hard drives before repair or disposal
- Change the default SNMP community strings
- Monitor and manage devices using a standard, secure management tool

## 3.12 Miscellaneous guidelines

- Departments must keep in mind possible additional requirements for complementary products or services, for example software development for barcoding systems or software interfaces for biometric devices.
- Make use of disposal services offered by OEMs for end-of-life products and used consumables.
- Enable power saving on all devices, including printers, MFPs and scanners. 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 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-2 security standard.
- Support is available for previous versions of operating systems, making it possible to maintain existing Departmental standards by allowing support for peripheral devices under a range of desktop operating

systems. For example an older printer should still be compatible with a brand-new PC with the latest OS, and conversely and new printer should support previous versions of the standard desktop OS.

- MFP and printer security:
  - As per SACSA guidelines, only non-classified communications may be done via unsecured channels such as fax machines (MFPs) available in the Peripherals domain.
  - Password-protected and encrypted communications must be used for the device's management interface.
  - Built-in hard drives must be securely erased according to accepted standards before disposing of or re-allocating the device.

# 4. Engagement guidelines

The Peripherals 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 Departmental standards

SITA recommends that Departments follow the best practice of defining internal ICT standards for procurement, e.g. standard desktop OS, printer/scanner make and model, database management system (DBMS), desktop devices (e.g. laptop make and model).

In order to establish legitimate Departmental standards, the following aspects must be addressed:

❖ Reasonable, documented business requirement per category (e.g. a user producing GIS maps needs a workstation with the appropriate performance and software tools, as well as a large-format printer)

❖ User profiles must be defined per category where applicable

❖ Products must be SITA-certified

❖ TCO calculation

❖ Installed base taken into account (e.g. existing system vs green-fields installation)

❖ Report from ICT division motivating the standard

❖ The standard must encompass as much of the Department's ICT environment as possible

❖ Approved by Department Accounting Officer

❖ Standard must be periodically reviewed (every 3–5 years)

### 4.1.3 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 products in the proposal. This is addressed in detail later in the document.

### 4.1.4 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.

## 4.2 Supplier guidelines

Where applicable, certified suppliers are required to adhere to the following normative standards when supplying products certified via the Peripherals 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 responsibility 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 Peripherals 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 270 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. Mono2, MFC4, Scanner1) 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 the 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). 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).

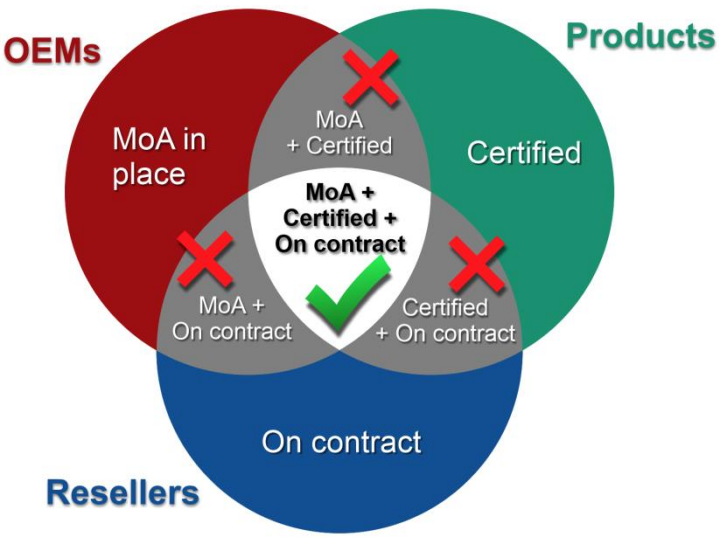



Figure 9: Requirements for supply to Government

- 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 Peripherals 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 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.

### 5.2.3 Additional best practices

- Where appropriate, FOSS operating systems and environments are supported by all products as approved via the technology certification process, and are compatible with mainstream open-source software. 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. using unsupported paper that damages a printer). 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 Peripherals technology domain supports the establishment of a transversal procurement vehicle for a baseline technology platform that should cater for at least 95% of Government's Peripherals 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. For requirements falling outside the 95%, Departments are encouraged to contact TAS for targeted technology advice.

A thorough analysis of user requirements must be done to ensure that a fit-to-purpose solution is procured from the Peripherals 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.

## More information 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 contact persons for product certification, advisory services and technology domain information:

| Name | Role | Contact details |
|---|---|---|
| Deon Nel | Technology consultation and certification | deon.nel@sita.co.za<br>012 482 2136 |
| Izak de Villiers | Technology consultation and certification | izak.devilliers@sita.co.za<br>012 482 2749 |
| Hlengiwe Mosokotso | Certification requests, Lab coordination and communication | tas@sita.co.za<br>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.<br>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.<br>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 / RT3). | | |
| **Substantiate:**<br>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:**<br>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. Printer / MFP), Item (e.g. MF1) and specific product offered in the proposal/quotation. | | |
| **Substantiate:**<br>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.<br>The individual product certificates for the offered products must be attached to this bid. | | |
| **Substantiate:**<br>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:**<br>Attach proof of supplier's OEM accreditation. | | |

| 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:**<br>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:**<br>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:**<br>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 Peripherals domain.

| Major solution components | Quantity | Unit Price (Excl VAT) | Nett Price (Excl VAT) |
|---|---|---|---|
| Basic device as specified | | | |
| Basic software (e.g. printer drivers or scanning capture software) | | | |
| Upgrades (e.g. paper trays, storage) | | | |
| Accessories (e.g. additional connectivity) | | | |
| Additional software (e.g. print management) | | | |
| Additional services (e.g. optimisation, integration, software installation, configuration 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: Requirements Checklists

In order to support Departments in specifying the appropriate technology solutions and devices, SITA has prepared Requirements Checklists for specific types of solutions. These can be downloaded from www.sita.co.za/prodcert.htm and filled in to document business needs.

SITA

## Requirements Checklist: Barcode Scanner

This checklist is to be used by Departments to document business requirements when publishing a request to industry for a barcode scanner or auto-ID solution. The checklist will help define the business requirements, enabling suppliers to provide informed solution designs and bid responses.

| Business requirements | | | |
|---|---|---|---|
| For example: "Capture assets within stores environment with a handheld device connected to Departmental wifi network." | | | |
| **Functionality required** (tick with ✓ where applicable) | | | |
| Integrated handheld device with scanner | ☐ | WiFi network connection | ☐ |
| Separate scanner (USB) + mobile device (tablet/laptop/phone) | ☐ | LTE network connection (no wifi available) | ☐ |
| Separate scanner (wireless) + mobile device (tablet/laptop/phone) | ☐ | Installation and training required (device-specific) | ☐ |
| **Technical requirements** | | | |
| Type of barcodes or other ID tags in use for assets (e.g. Code 39 barcodes / NFC tags) | | | |
| Network connection to back-end system (e.g. WiFi or LTE/3G to NT LOGIS) | | | |
| Data bundle required for LTE devices? | | | |
| Network configuration required? (e.g. WiFi setup) | | | |
| Portability/mobility requirements: e.g. 8 hours battery life to support full-day shift | | | |
| List other standards/requirements that must be adhered to/met | | | |
| Describe unique technical requirements (if any) | | | |
| **Integration and technology requirements** | | | |
| Client-side application used for scanning (e.g LOGIS) | | | |
| List requirements of scanning app (screen, RAM, connectivity, etc.) | | | |
| Server-side system for storing and processing scanned data (if other than LOGIS) | | | |
| List requirements of server system (API, protocols, connectivity, etc.) | | | |
| System integration: does the solution need to integrate with an existing logistics system? (e.g. National Treasury LOGIS) | | | |
| Does this system have any mimimum technology requirements? (e.g. device specifications: CPU, RAM, screen size) | | | |

# Requirements Checklist: Document Scanner

This checklist is to be used by Departments to document business requirements when publishing a request to industry for a document scanner or paper capture solution. The checklist will help define the business requirements, enabling suppliers to provide informed solution designs and bid responses.

| Business requirements | | | |
|---|---|---|---|
| For example: "Capture paper documents within records environment; approximately 100,000 pages to be scanned." | | | |
| **Description of documents to be scanned** | Tick with ✓ where applicable) | | |
| A4 paper | ☐ | Plain bond paper | ☐ |
| A3 paper | ☐ | Thick paper or cardboard | ☐ |
| Small paper (A5) – specify: _____ | ☐ | Thermal or smooth/thin paper | ☐ |
| Larger paper (A2+) – specify: _____ | ☐ | Colour documents | ☐ |
| Specialised documents (e.g. cards, ID books, maps) | ☐ | Monochrome (B&W) documents | ☐ |
| Scan single-sided / double-sided | ☐ | | |
| **Data/content types** (information to be captured from the paper) | Tick with ✓ where applicable) | | |
| Laser printed | ☐ | Coloured backgrounds | ☐ |
| Handwritten | ☐ | Coloured forms | ☐ |
| Barcodes | ☐ | Watermarks, patterned background | ☐ |
| Dot matrix / thermal prints | ☐ | Graph paper | ☐ |
| Standard forms with filled-in information | ☐ | Faded / faint content | ☐ |
| Black and white | ☐ | Other: specify _____ | ☐ |
| Colour or single-colour (non-black) | ☐ | _____ | |
| **Functionality required** | Tick with ✓ where applicable) | | |
| Optical character recognition (OCR) | ☐ | Colour drop-out? | ☐ |
| Intelligent character recognition (ICR) – handwriting | ☐ | Mixed paper sizes/thicknesses? | ☐ |
| Optical mark recognition (OMR) | ☐ | Mixed quality or type of content? | ☐ |
| Electronic content management (ECM) | ☐ | Flatbed (for large/non-standard/awkward docs) | ☐ |
| **Process requirements** | Tick with ✓ where applicable) | | |
| Total amount of documents to be scanned (estimated pages) | | | |
| Timeframe for scanning (deadline for back-scanning) | | | |
| Time limitations for scanning (e.g. only mornings, or 2 days a week) | | | |
| Batch/archival/back-scanning or daily business-process scanning? (transactional vs. bulk) | | | |
| Document preparation required? (Staples, paperclips, remove from files, etc.) | | | |
| Centralised or distributed scanning? | | | |

# Annex C: 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 Peripherals 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. consumables for a printer)
- 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 Peripherals Technical Specifications at www.sita.co.za/prodcert.htm.

# Annex D: Solution Checklist: Peripherals

This annex specifies the bundled and optional accessories for the Peripherals domain in the form of a checklist to be used by Departments to help specify peripheral 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 RT3, 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.

| Printers | |
|---|---|
| **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<br>❖ Set of consumables<br>❖ Warranty and SLA (3-year on-site with specified repair time)<br>❖ Standard power and interface cables<br>❖ Documentation<br>❖ Drivers for standard operating systems<br>❖ Packaging and delivery to client site | ❖ On-site installation<br>❖ Upgrades to warranty (beyond default 3-year on-site)<br>❖ Non-standard accessories, e.g. additional paper trays, finishers, additional cables, etc. |

| Multifunction 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<br>❖ Set of consumables<br>❖ Warranty and SLA (3-year on-site with specified repair time)<br>❖ Standard power and interface cables<br>❖ Documentation<br>❖ Drivers for standard operating systems<br>❖ Packaging and delivery to client site | ❖ On-site installation<br>❖ Upgrades to warranty (beyond default 3-year on-site)<br>❖ Non-standard accessories, e.g. additional paper trays, finishers, additional cables, etc. |

| Scanners | |
|---|---|
| **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<br>❖ Set of consumables<br>❖ Warranty and SLA (3-year on-site with specified repair time)<br>❖ Standard power and interface cables<br>❖ Documentation<br>❖ Drivers for standard operating systems<br>❖ Packaging and delivery to client site | ❖ On-site installation<br>❖ Upgrades to warranty (beyond default 3-year on-site)<br>❖ Non-standard accessories, e.g. additional software, interfaces, imprinters, etc. |

| Digital cameras | |
|---|---|
| **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<br>❖ Warranty and SLA (**1-year carry-in** with specified response time)<br>❖ Standard flash memory card or internal storage as specified<br>❖ Lens as specified (**Cam_Sys2 is specified without a lens**)<br>❖ Rechargeable battery and charger<br>❖ Standard power and interface cables<br>❖ Carry bag and lens cap<br>❖ Shoulder/wrist strap<br>❖ Documentation<br>❖ Drivers and supporting software for standard operating systems<br>❖ Packaging and delivery to client site | ❖ On-site installation<br>❖ Upgrades to warranty (beyond default 1-year carry-in)<br>❖ Non-standard accessories, e.g. additional storage, carry bags, lenses, tripods, flashes, etc. |

| Auto-ID 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<br>❖ Warranty and SLA (3-year on-site with specified repair time)<br>❖ Standard power and interface cables (charging/docking cradles for wireless devices)<br>❖ Documentation<br>❖ Drivers and supporting software for standard operating systems (if applicable)<br>❖ Packaging and delivery to client site | ❖ Applications software, integration into existing or new system<br>❖ On-site installation<br>❖ Upgrades to warranty (beyond default 3-year on-site)<br>❖ Non-standard accessories, e.g. additional interfaces, consumables, media types, etc. |

| Consumables | |
|---|---|
| **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<br>❖ Warranty and SLA (**2-year on-site** with specified response time)<br>❖ Standard power and interface cables (if applicable)<br>❖ Drivers and supporting software for standard operating systems<br>❖ Packaging and delivery to client site | ❖ On-site installation<br>❖ Upgrades to warranty (beyond default 1-year carry-in) |

| Device management tools | |
|---|---|
| **Included with Base Unit** | **Not Included with Base Unit** (client to specify) |
| ❖ Typically a per-device, per-user or per-server licence. | ❖ Additional functionality which is licenced separately. |

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

# Annex E: 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 SC-ITSM. |
| 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. Components from third-party manufacturers cannot be certified directly via the TPC, but are offered by OEMs 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. Prn_Mono2, Scan_Doc4. A product must be offered at Item level. Multiple products may be offered for each Item. Items are organised into Categories, e.g. Printers, Scanners, Cameras, 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. |
| Peripheral | A device attached to a computing system that enables input and output of information |

| 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:<br>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.<br>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.<br>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.<br>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.<br>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 Peripherals domain:<br>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. |