Deployment Guidelines:
Servers and Storage

Version:	2.0
Date:	2019-01-11

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: Servers and Storage
Document No: **eNSQS-00148**
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 HOD: Norms Standards and Quality National Consulting Services Division	14/01/2019 Date
Izak de Villiers Senior Specialist: TAS	14/1/2019 Date

Foreword

This document forms part of a Servers and Storage best practices guideline and solution selection process enabling cost-effective procurement and deployment of ICT by Government and SITA using transversal procurement processes. 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 Servers and Storage (e.g. Transversal Contracts 2003 or 2013). **Complete, turnkey** solutions are in view, including all required components and associated services (e.g. consultation, design, supply, installation, training, support and maintenance).

Contents

Tables

Figures

1. Introduction and background

This Deployment Guide recommends best practices for specifying solutions from the Servers and Storage technology domain (comprising Tower, Rack and Blade servers, and various types of storage, including Primary, Secondary and Archiving), and provides guidelines, standards and advice for the effective selection and deployment of appropriate technologies and solutions. The main purpose of the Deployment Guide is to inform end users about best practices and cost-effective, optimal utilisation of available solutions.

These guidelines are not intended to replace Departmental ICT policies and processes, but complement and augment them, while focussing on adding value during the entire ICT lifecycle. Applicable guidelines should be used in conjunction with other related documentation, including any relevant internal policies, Transversal Contract Engagement Models, contract conditions, definitions and technical specifications. A comprehensive list of definitions is provided in the Annex for reference.

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 the Annex, to be incorporated into Requests for Quotation/Proposal.

Experience with Government requirements and requests for quotation shows that many Departments copy specifications from industry-supplied information, instead of writing their own. This practice typically compromises fairness and an adequate definition of the actual business requirement, whereas the SITA process requires unbiased specifications and an emphasis on business needs.

Technology Advisory Services (TAS) publishes these deployment guidelines as part of a SITA initiative to enable efficient and cost-effective use of ICT in Government. The guidelines are an output of the unit's standard research, evaluation and consultation processes, and are developed in collaboration with clients, suppliers and manufacturers.

Both **normative** and **informative** guidelines are documented in the guide. Informative guidelines point out best practices and other helpful information, while normative guidelines **must** be followed by Departments. Any deviations from normative guidelines may result in audit findings.

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: new transversal bids for Servers and Storage solutions have been published, and the resulting contracts will establish the following:
  - Master Agreement: Servers and Storage contract (Contract 2003 or 2013)
  - Engagement Model: Servers and Storage contract (Contract 2003 or 2013)
- Processes and documents:
  - Technology Certification Process (eIRPL-00001), version 3.3, November 2018

- SITA Product Certification: OEM Memorandum of Agreement (eIRPL-00002), version 1.6, November 2018
- 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

1.2 Standardisation

Standardisation helps Government to achieve 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:

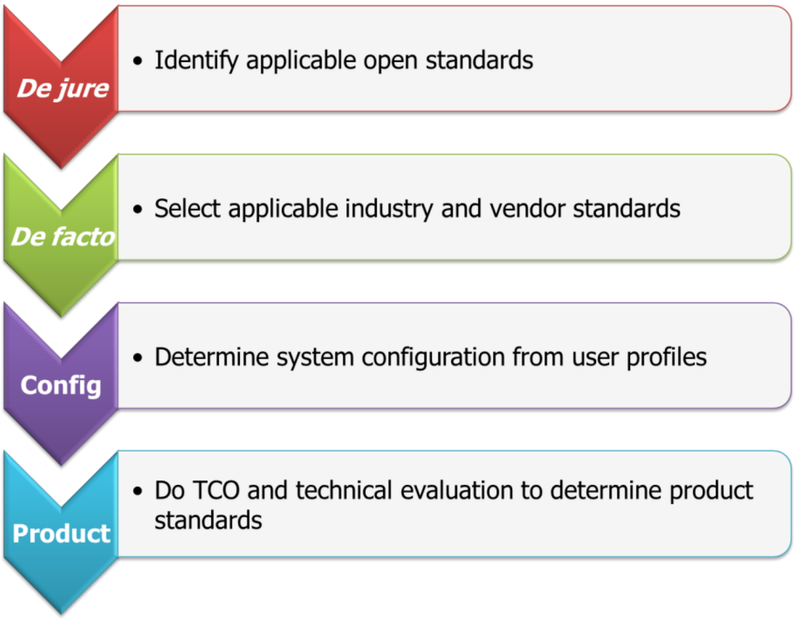

De jure
• Identify applicable open standards
De facto
• Select applicable industry and vendor standards
Config
• Determine system configuration from user profiles
Product
• Do TCO and technical evaluation to determine product standards

Figure 1: Standards selection process

- 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 and 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.
- Generally-accepted vendor and industry standards (*de facto*): These are not open standards, but they are so widespread that industry must to conform to them to meet interoperability requirements. Operating systems such as Microsoft's Windows Server 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 formal standardisation. Other examples of this are Android in the mobile OS space, or Dante in the AVCT domain.
- **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 configuration file can be used to configure a population of servers uniformly to reduce system management effort and costs.
- **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 operations 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 or hardware configurations. Departments are encouraged to standardise down to product level to reduce complexity and improve interoperability within the Department.

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

1.3 Design principles

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

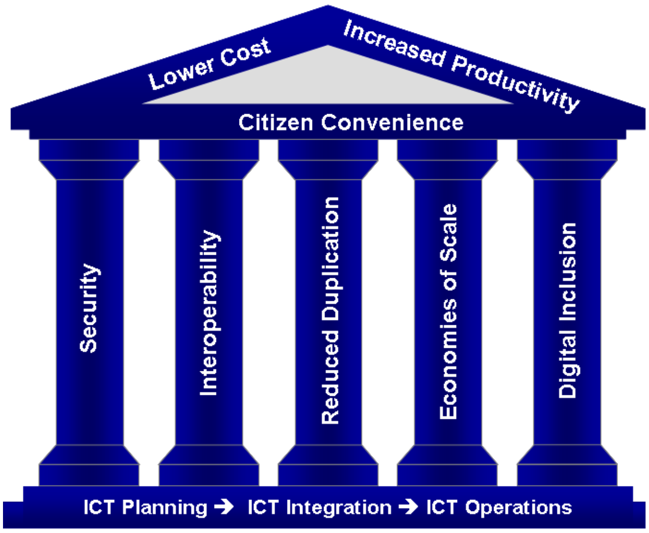


Figure 2: ICT House of Value

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

1.4 Processes

1.4.1 Product certification

According to the SITA Act, the Agency must certify ICT goods and services to ensure that they conform to ICT standards, security 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.

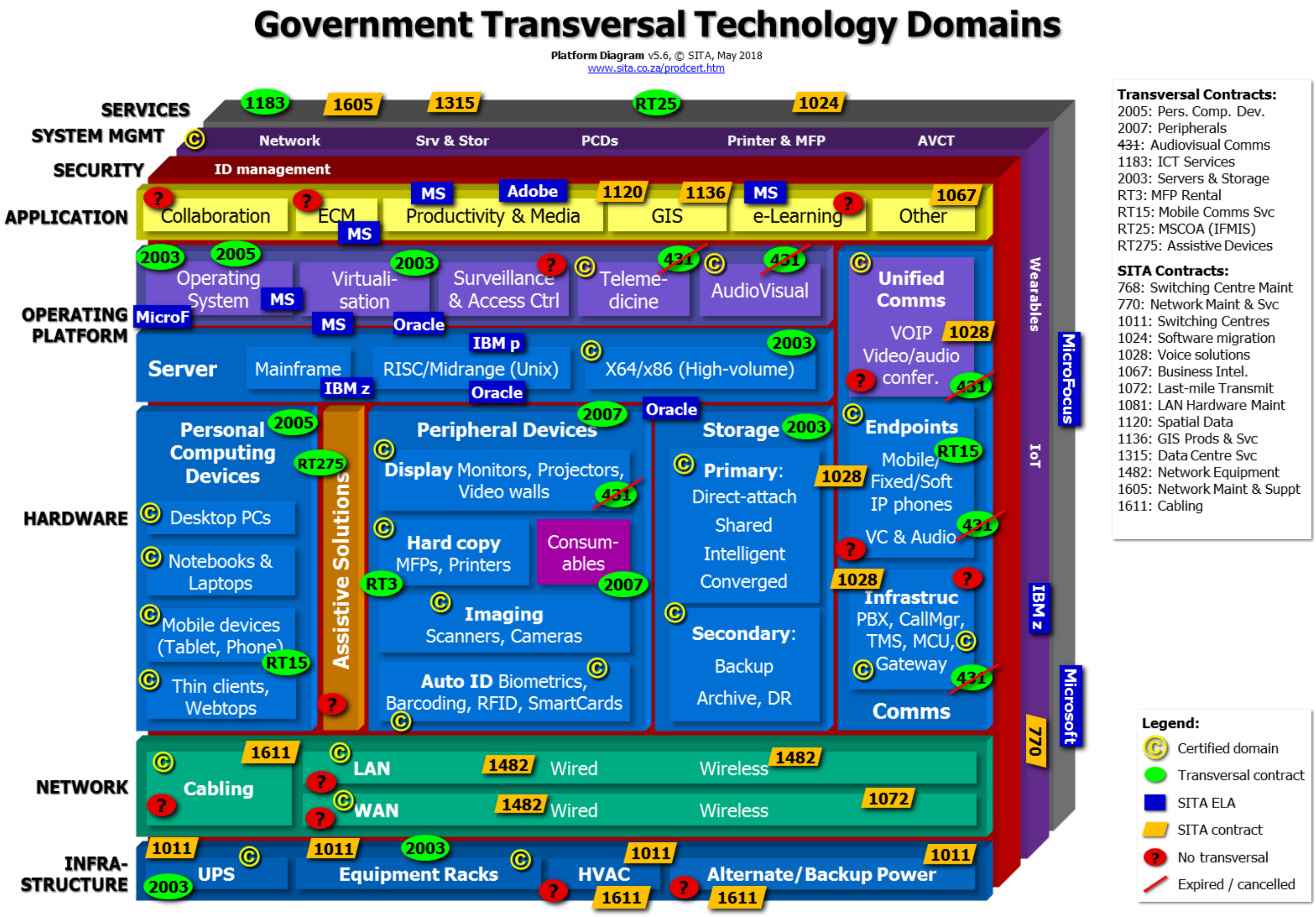
Domain	Components
Personal Computing Devices	Desktop PCs, Mobile PCs, Desktop displays, and Mobile devices (Tablets, Smartphones, eReaders).
Peripherals	Printers, Multifunction devices, Scanners, Digital cameras, Auto-ID (Barcoding, Card devices), Optical storage (DVD duplicators), Small peripherals and Consumables.
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 and 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, Cable ducting, trenching and routing.

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 a Servers and Storage solution for a Department. These PCs must be certified according to the requirements of the PCDs domain, even though the broader solution is procured via the Servers and Storage 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.



Transversal Contracts:

2005:	Pers. Comp. Dev.
2007:	Peripherals
~~431~~:	Audiovisual Comms
1183:	ICT Services
2003:	Servers & Storage
RT3:	MFP Rental
RT15:	Mobile Comms Svc
RT25:	MSCOA (IFMIS)
RT275:	Assistive Devices

SITA Contracts:

768:	Switching Centre Maint
770:	Network Maint & Svc
1011:	Switching Centres
1024:	Software migration
1028:	Voice solutions
1067:	Business Intel.
1072:	Last-mile Transmit
1081:	LAN Hardware Maint
1120:	Spatial Data
1136:	GIS Prods & Svc
1315:	Data Centre Svc
1482:	Network Equipment
1605:	Network Maint & Suppt
1611:	Cabling

Legend:

©	Certified domain
🟢	Transversal contract
🟦	SITA ELA
🟨	SITA contract
?	No transversal
/	Expired / cancelled

Figure 3: Platform Diagram

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

1.4.2 Technology evaluation and management processes

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

Technology evaluation process

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

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

2) **TCO:** Calculation of technology component of TCO based on supplied cost information and component pricing.

3) **Physical verification phase:** Laboratory tests and/or demonstrations of products and solutions (depending on domain and category).

   a) Validate supplied information via system tests or OEM documentation.

b) Verify interoperability via compatibility tests or OEM/ISV certifications.

c) Performance benchmarks using industry-standard benchmarks as well as methodologies developed in-house (depending on domain).

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 the 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 Servers and Storage suppliers for input before implementation. All changes to the technology specification must be used as an input to any procurement or pricing exercise, which ensures that Government has a fair basis for performing in-house price and and cost analyses.

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 included technology domains.

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

2. Overview of Servers and Storage domain

The purpose of the technology domain is to specify and certify suitable products for deployment within Government, in support of any procurement vehicle established in this space (e.g. Transversal Contract 2003 or 2013).

2.1 Scope

The Servers and Storage technology domain comprises the following categories and technology types, which inform the building blocks to be used to create Servers and Storage solutions:

Category	Technologies
Servers	1- to 8-socket tower/rack servers and blade servers, including building blocks for virtualised, hyperconverged and software-defined solutions.
Primary storage	Direct-attached and shared intelligent storage arrays, including building blocks for NAS and SAN solutions.
Secondary storage	Tape automation and disk-to-disk solutions for backup and archiving solutions
In addition to the categories above, Srv&Stor solutions usually incorporate building blocks from the Infrastructure domain, which includes the following components:	
UPS	Line-interactive UPS On-line UPS

Category	Technologies
Server racks	Standard 19" equipment racks and environmental racks

Table 2: Categories in the Servers and Storage domain

Detail specifications for all these categories and technologies and are available for download from www.sita.co.za/prodcert.htm.

Note: The current certification process for Servers and Storage does not cater for RISC, non-X64 or other specialised computing architectures, which are typically procured via *ad hoc* tenders.

2.2 Domain goals and criteria

The following overall goals and evaluation criteria are integrated into the design of the technical specification. Inputs from component manufacturers (e.g. CPUs, HBAs and disk drive components), 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 5-year on-site warranty and 8-hour **repair** 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. 10Gb Ethernet and Fibre Channel).
    - Processing capabilities (e.g. processor speed and memory capacity).
    - Upgrade options and accessories (e.g. storage, connectivity, management systems).
    - Security capabilities (e.g. physical locks, encryption, secure management).
    - Compatibility and interoperability (both hardware and software) via ISV and OEM certifications (e.g. Microsoft, Red Hat, VMware).
    - 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 Solution design

The Servers and Storage domain supports the acquisition of **complete, turnkey solutions**, including any type of virtual, hyperconverged or software-defined solution that may be required by Government. Associated services, components, accessories, partner models and accreditation mechanisms form part of the domain design.

The domain caters for complexity at both ends of the spectrum: a simple product acquisition may be done (e.g. purchasing just a tape library or UPS), but more often clients require a fully functional turnkey solution such as an equipment rack populated with servers, storage and UPS, with all services, technologies and infrastructure fully integrated.

The diagram illustrates the relationship between domain components or products and the services rendered by suppliers to arrive at a full solution satisfying end-user requirements. The process flow starts with a detailed client requirements specification, after which technology components are integrated into a design by the supplier, and delivered as a fully working solution.

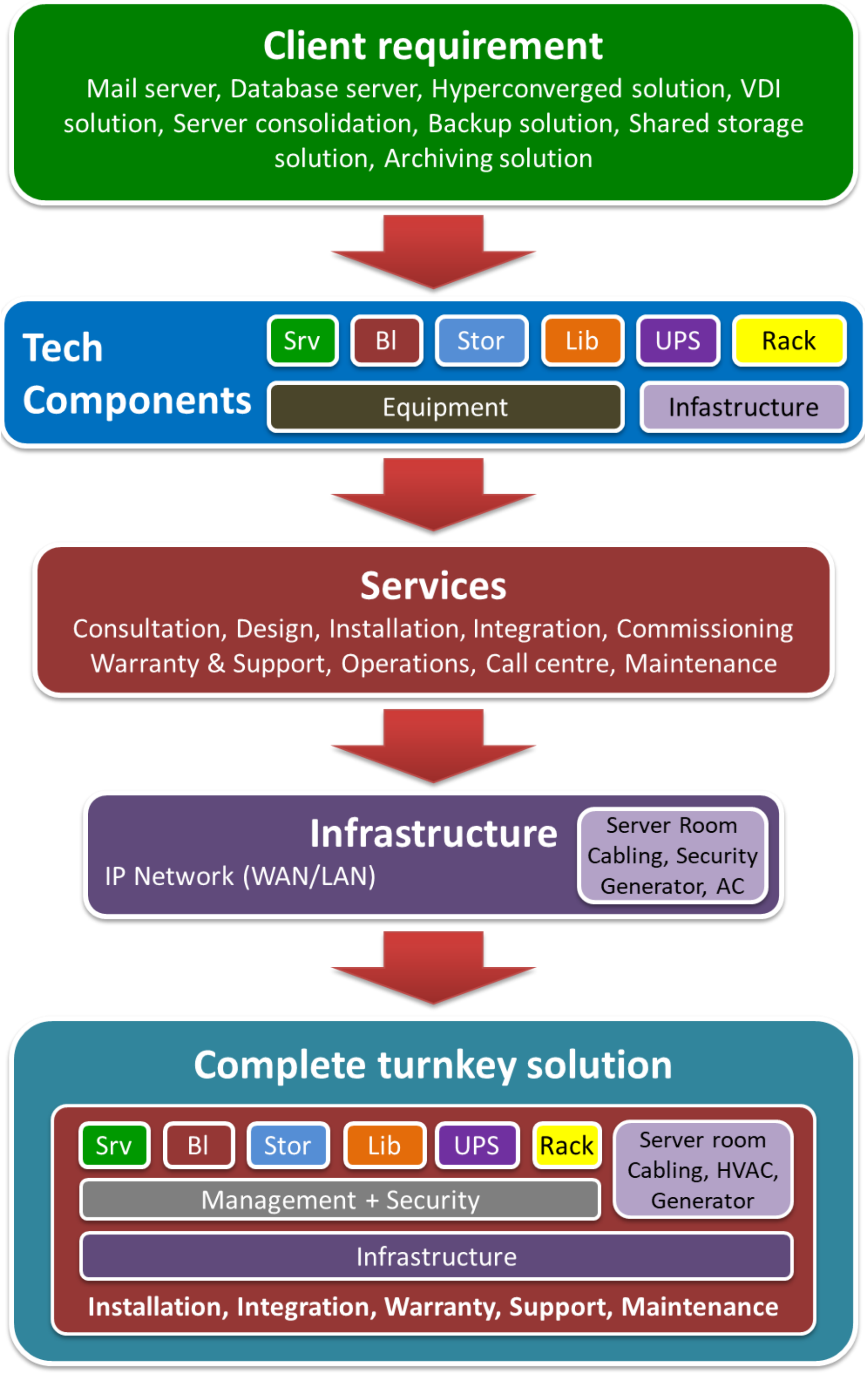

Client requirement
Mail server, Database server, Hyperconverged solution, VDI solution, Server consolidation, Backup solution, Shared storage solution, Archiving solution
Tech Components
Srv
Bl
Stor
Lib
UPS
Rack
Equipment
Infastructure
Services
Consultation, Design, Installation, Integration, Commissioning Warranty & Support, Operations, Call centre, Maintenance
Infrastructure
IP Network (WAN/LAN)
Server Room Cabling, Security Generator, AC
Complete turnkey solution
Srv
Bl
Stor
Lib
UPS
Rack
Server room Cabling, HVAC, Generator
Management + Security
Infrastructure
Installation, Integration, Warranty, Support, Maintenance

Figure 4: Turnkey solution focus

As can be seen in the diagram, technical requirements and components make up only a small part of the total solution. Complete, fully functional turnkey solutions are in view in all cases. Contractors must take responsibility for the entire end-to-end solution, including consultation, design, installation, service and support.

The following diagram illustrates the relationships of the various phases of a Servers and Storage project. The customer's solution requirements are central, and must be prioritised at all times.

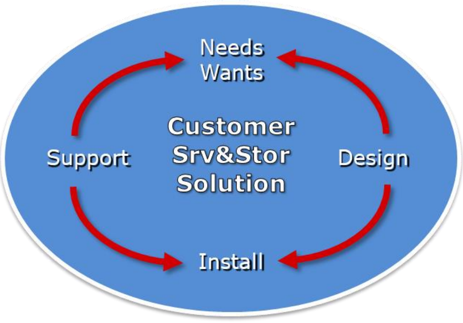


Figure 5: Customer centrality

2.4 Domain components and usage profiles

The components of the Servers and Storage 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 Servers and Storage solution is the **business requirement**, or how the system will be used. To keep costs as low as possible (in line with the PFMA), a general principle is to select the smallest available system that supports the required functionality.

The ICT-based components listed below will form part of the technology management cycle (i.e. be subject to product certification and Tech Updates). The list of categories and technologies may be expanded or adapted over time, depending on SITA and government requirements. Any changes will be made in collaboration with Government and industry, and will only be implemented once approval has been given by the relevant GITO Council authority.

2.4.1 Tower and rack servers

Item	Description	Usage profile
Srv1	Entry-level 1-socket server	Entry-level 1-socket multi-core X64 tower/rack-mount system
Srv2	Entry-level 2-socket server	Entry-level 2-socket multi-core X64 tower/rack-mount system
Srv3	Advanced 2-socket server	Advanced 2-socket multi-core X64 rack-mount system with redundant storage, power and cooling
Srv4	Advanced 4-socket rack server	Advanced 4-socket multi-core X64 rack-mount system with redundant storage, power and cooling
Srv5	Advanced 8-socket rack server	Advanced 8-socket multi-core X64 rack-mount system with enterprise-level RAS features and redundant storage, power and cooling

Table 3: Tower and rack server usage profiles

2.4.2 Blade servers

Item	Description	Usage profile
Bl1	Blade server chassis	Blade server chassis, including redundant power, cooling, connectivity and accessories
Bl2	2-socket blade server	Advanced 2-socket multi-core X64 blade server
Bl3	4-socket blade server	Advanced 4-socket multi-core X64 blade server

Table 4: Blade server usage profiles

2.4.3 Direct-attached storage

Item	Description	Usage profile
Stor1	Direct-attached storage (DAS) array	Controllerless direct-attached storage array (JBOD)
Stor2	Intelligent direct-attached storage (DAS) array	Direct-attached storage array with on-board storage controller

Table 5: Direct-attached storage usage profiles

2.4.4 Intelligent shared storage

Item	Description	Usage profile
Stor3	Entry-level intelligent shared storage array	Entry-level / value multi-protocol shared storage array with software and connectivity options
Stor4	Midrange intelligent shared storage array	Midrange multi-protocol shared storage array with software and connectivity options
Stor5	Advanced intelligent shared storage array	Advanced multi-protocol shared storage array with software and connectivity options
Stor6	Intelligent shared storage controller/front end	Multi-protocol shared storage front end for existing or third-party disk

Table 6: Intelligent shared storage usage profiles

2.4.5 Tape automation

Item	Description	Usage profile
Lib1	Entry-level tape library/autoloader	Entry-level tape library or autoloader for backup and archiving, single tape drive, 8 slots
Lib2	Midrange tape library	Midrange tape library for backup and archiving, 1-4 tape drives, 30 slots
Lib3	Advanced tape library	Advanced tape library for backup and archiving, 2-8 tape drives, 60 slots

Table 7: Tape automation usage profiles

2.4.6 Disk-to-disk backup

Item	Description	Usage profile
DtD1	Entry-level disk-to-disk backup solution	Entry-level disk-to-disk backup/archival solution with optional tape library emulation, 5TB raw storage
DtD2	Midrange disk-to-disk backup solution	Midrange disk-to-disk backup/archival solution with optional tape library emulation, 10TB raw storage
DtD3	Advanced disk-to-disk backup solution	Advanced disk-to-disk backup/archival solution with optional tape library emulation, 40TB raw storage

Table 8: Disk-to-disk backup usage profiles

2.4.7 Services

Services that can be rendered as part of a Servers and Storage solution include, but are not limited to, the following:

- Consultation
- Site inspection
- Design and system architecture
- Detail requirements specification
- Development and programming
- Installation
- Integration
- Commissioning
- Training
- Support
- Maintenance
- Operations
- System management and administration

2.4.8 Infrastructure components

In addition to technology and service components, the following infrastructure may be required as part of a complete solution:

- Network cabling
- Cooling and ventilation (installation and control)
- Surveillance and access control (installation and control)
- UPS and other power requirements (including electrical work)
- Structural modifications (if required in the facility)

For network cabling existing transversal contracts must be used where possible, while other components and/or integrations may be quoted via RFP/RFQ according to Treasury regulations, in association with Public Works.

2.5 Domain value-adds

The following domain features add value to Government ICT acquisition processes by mandating minimum requirements that support local ICT initiatives and requirements.

- Because of the critical nature of Government's communications infrastructure, very stringent technical and quality standards are specified for all devices. Manufacturing and environmental standards ensure high-quality solutions that support Government reliability and environmental drivers.
- Compatibility with network standards and protocols such as DNS, DHCP, IPv4 and IPv6.

- A strong emphasis is placed on systems management, allowing support staff to remotely monitor, configure, update and troubleshoot devices, saving on labour and travelling costs, and minimising downtime.
- Countrywide, 5**-year on-site warranty** with 8-hour **repair** SLA for all systems (Zone A only; Zones B and C extend the repair time to 16 and 24 working hours respectively). To further ensure maximum productivity, SLA upgrade options are also mandated for all products, which can be procured at the client's discretion.
- Certified products, components and solutions are available for direct procurement from a selection of accredited suppliers.
- A full range of upgrade options, components and accessories is available with each solution. This includes communications and media options, software, accessories, etc. Suppliers are required to build complete solutions for Departments with these options.
- Compatibility with standard operating systems and environments (including Windows, Linux, Vmware, etc.)
- Software licences for all basic functionality as specified are included in the Base Price. Additional software functionality (e.g. hypervisor or OS licences) may be licensed via component price lists as submitted by the OEM during certification.
- Firmware updates for all components for the duration of the product warranty, at no cost to the user.

2.6 Bundled accessories and services

Each Servers and Storage Item and/or solution is specified as a **fully working configuration** with a minimum set of mandatory bundled accessories and services. For example, all solutions must be bundled with the minumum SITA-specified configuration of CPU, RAM and support, including standard cables, rack mountings, etc. None of these standard components may be left out by suppliers, but Government may substitute the default components with alternatives or upgrades if required (e.g. a larger CPU or RAM configuration, a server with rack-mount instead tower configuration, or a separate KVM solution.) Departments must ensure that the business requirement is stated in full in the RFQ/RFP to ensure that the supplier's proposed solution includes all components for a fully working, turnkey solution. This includes additional non-standard requirements such as upgrading the standard support SLA). The Annex has additional details on this.

The specification prevents suppliers from quoting or delivering incomplete solutions (e.g. leaving out required cables or components), and suppliers are mandated to deliver and working, turnkey solutions.

Mandatory support SLA: all solutions must be bundled with the standard specified **on-site support SLA** included in the price. To ensure the lowest possible TCO for Government, the warranty and support **cannot** be unbundled from the price.

2.6.1 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. Required turnaround times for response and repair differ per zone, resulting in the following 3 SLA levels:

Zone A – repair within 8 office hours: The entire Gauteng Province, as well as within 50km from major cities or Provincial capitals, i.e. Cape Town, Port Elizabeth, East London, Bisho, Bloemfontein, Durban, Mmabatho, Polokwane, Kimberley, Pietermaritzburg, Ulundi, Witbank and Nelspruit.

Zone B – repair within 16 office hours: In or within 50km from major towns, i.e. Welkom, Umtata, George, Grahamstown, Thohoyandou, Rustenburg, Klerksdorp, Ermelo, Standerton, Ladysmith, Oudtshoorn, Richards Bay, Saldanha, Upington, Worcester, Potchefstroom and Beaufort West.

Zone C – repair within 24 office hours: All towns and rural Zones not included in Zone A and Zone B where services may be required.

In addition to the 8/16/24-hour repair time, the specifications require a **4-hour response**, during which period the service provider **must** contact the client and acknowledge receipt of the call.

3. Servers and Storage selection guidelines

3.1 Business requirement

The most important principle in deploying any ICT-based system, including servers and storage, is that the **end-user requirement** must determine the type of system or doluyion that must be procured. This means that the solution must be able to perform all the required functionality in the end-user environment (e.g. a database server for a specified number of users and performance level, or a shared storage solution with a specified capacity and latency).

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 solution will bring to the end-user's process or function.

The basic philosophy when specifying any type of device or system 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 in terms of the Constitution.

3.2 General principles

The following general principles must be followed to specify, evaluate and select solutions.

- Specify and deploy **fit-for-purpose** solutions and technologies for specific business requirements (e.g. mobility or performance). Fit-for-purpose solutions enable efficiency and reduce TCO.
- 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 as per NT guidelines, is in force.
- Detail product specifications (e.g. CPU clock speed in Ghz, exact dimensions and weight) should **not** be used to define an end-user requirement. The business need must be defined based on actual usage requirements.
- The technology domain focusses on enterprise-level devices: this means that manageability, compatibility and longevity of systems and accessories are maximised while TCO is minimised. Systems designed for a retail or consumer environment will not meet this requirement, and will not be certified.
- Bundled services: ensure that the standard services are included in the solution specification. These include initial training, and on-going support and maintenance for the SLA period.
- Where possible, Departments should standardise on brand and model to reduce complexity, minimise TCO and maximise interoperability, business continuity and user productivity. In the case of such a standard being established in a Department, brands **should** be specified as part of the request. Where integration is required with existing technology or systems, brands **must** be specified to ensure a complete and adequate solution design.

3.3 System management tools

These tools or systems can enable Departments to contain costs by allowing accurate tracking, control and costing of ICT systems. Departments must stipulate exactly which products or devices 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. This results in a higher TCO, which is in contravention of the cost-effectiveness mandate of the Constitution.

3.4 Security

The security architecture of any ICT system is a vital component of the total solution. Standards are in place for security, but practical measures also need to be taken (e.g. access control), and the configuration of devices must be done in accordance with industry best practices.

Possible threats or risks include unauthorised access to systems via the built-in IPMI network management interface that is installed in all server devices.

The following security recommendations apply to all network-attached devices and systems:

- Enable user authentication or access control
- Set a strong administrator password
- Disable unused ports and protocols (e.g. FTP, POP)
- Set passwords for all remotely accessed services
- Disable USB ports if they are not used
- Enable hard drive encryption
- Securely erase all storage devices (hard drives, solid state storage) before repair or disposal
- Change the default SNMP community strings
- Monitor and manage devices using a standard, secure management tool

3.5 General guidelines

- Departments must keep in mind possible additional requirements for complementary products or services, for example software development to enable integration with existing networks/systems.
- To ensure completeness of response by suppliers, specify whether the solution is a green-fields scenario, or whether integration will be required.
- Make use of disposal services offered by OEMs for end-of-life products.
- UPS recommendation: for environments with unstable power or with a large number of mission-critical devices, a suitable UPS must be deployed to support Servers and Storage solutions. UPSs for these requirements are certified via the Infrastructure domain.
- To ensure stable power for AVCT solutions, equipment racks must be properly electrically earthed as required by South African regulations.

- 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 string, as per Departmental/Government standards. 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 in terms of drivers for older devices. When procuring any peripheral device, Departments must specify which OS will be used to ensure driver support.
- Device 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.
  - All hard drives and other storage media must be securely erased before disposing of or re-allocating the device.

4. Engagement guidelines

The Servers and Storage domain specifies minimum requirements in terms of service delivery, security, response 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 the Annex 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 product 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.
- In cases of complex solutions, a thorough needs analysis process must be followed prior to publishing an RFP/RFQ to the panel of suppliers. This must include at minimum an indication of high-level business requirements. Site inspections by suppliers, a preliminary design, and a "reality check" may need to be included.
- For complete systems or solutions, the RFP/RFQ must cover at least the following:
  - 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. A basic SLA should be defined up front in the RFQ.
  - Maintenance of solution (both preventative and reactive). A regular preventative maintenance cycle should be stipulated where possible.
  - Required warranty, maintenance and support for the solution (both preventative and reactive).
  - Possible future upgrades with open standards-based interfaces.
- In the case of installed turnkey solutions, the supplier's proposal must include at least the following elements:
  - Complete solution design, including equipment, rack layout, connectivity, system integration and management.
  - A complete list of materials, including which of the existing infrastructure and components would need to be upgraded or replaced.
  - Support and maintenance proposal.
  - High-level project plan including the following phases:
    - Installation and configuration.
    - Integration.
    - Commissioning.
    - Training
- Complete pricing schedule incorporating a breakdown of all mandatory and proposed cost elements.
- Existing infrastructure and environment must be fully documented in the RFP/RFQ, or suppliers must be given the opportunity to do a site inspection. Details that must be documented per site include:
  - Drawings and measurements of the site (e.g. server room/data centre).
  - Type, number and position of network points.
  - Number and position of power outlets.

  - Availability of and access to site for installation services (both daytime and after hours), and the criticality of the site's current services (can it be taken off-line for the required installation time?).

- Any customer-furnished equipment or third-party equipment in the facility.

- Future-proofing of the required solution must be planned for to ensure the maximum value for the investment, as well as to guarantee interoperability with future technologies and protocols.

- Selection of the most suitable alternative must based on the lowest TCO calculated using the user requirement as input.

- Departmental standards should be used to expedite procurement of approved devices, while only exceptions (deviations from the standard) need to be explicitly motivated and approved by internal ICT committees.

4.1.2 Sizing and performance of solutions

- As with reliability and performance, the configuration and operational parameters of a system largely determine TCO, or cost-effectiveness. Capital costs and on-going costs (consumables, service, support, etc.) vary widely based on many factors. Licensing costs for additional required functionality (e.g. additional software functionality) must also be calculated. All these factors must be incorporated in the requirement to ensure a real-world comparison of total cost. Clients are encouraged to do a multi-year TCO comparison (a minimum of 5 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. For example, a web server has a different set of performance criteria from a database server, which differs in turn from an application server or a terminal server.

- Existing and planned network infrastructure must be taken into account when specifying the solution.

- Departments should specify storage capacity requirements in terms of **usable** capacity, and not raw capacity. There are significant differences in the way different vendors utilise raw disk capacity to add value to storage solutions. Therefore, raw capacity is not a realistic guideline. **Suppliers must also take note of this fact**, quoting all storage in usable terms, not raw terms.

- Storage performance is often related to the number of hard drive spindles in the system. Therefore, the lowest-cost solution that provides the required capacity may not always be the right solution. Departments may need to deploy a larger number of spindles to achieve the desired performance level. Solid-state technologies will alleviate some of these issues going forward.

- X64 servers are typically under-utilised, with activity levels of 20% and below on average. Consolidation of servers via virtualisation can address this inefficiency by deploying fewer servers that are utilised at higher rates.

- Best practice dictates that servers must be fully populated with CPUs up front, as adding additional CPUs at a later date is typically not supported by availability and compatibility constraints.

- The choice of hard disk type (NL-SAS, SAS or SSD) should be based on application-specific variables: e.g. mission-critical vs. high-performance vs. large-capacity and low-cost. SSD and SAS drives are more costly, but offer higher performance and reliability than NL-SAS. NL-SAS, on the other hand, offers higher capacity for lower cost.

- Redundant connectivity for storage and inter-server communication is recommended to ensure maximum reliability of the solution. Redundancy must also be specified for power and storage subsystems.

- When proposing a solution, suppliers must provide a complete list of all SITA-certified Items. This is addressed in detail later in the document.

4.1.3 Blade servers

- Blade server solutions must be designed with network requirements in mind, as a fully-populated blade enclosure could require several dozen new network and storage connections (e.g. 1 blade server may have up to 4 network interfaces and 4 storage interfaces).
- Best practice is to procure the full blade infrastructure (blade enclosure fully populated with power supplies, fans, connectivity, etc.) up front, instead of populating the enclosure as blades are added.

4.1.4 Equipment racks

- 19" equipment racks must be populated according to weight, taking rack load-bearing limits into account. Heavier devices (e.g. UPS) should be installed at the bottom of the rack.
- The load-bearing capacity of floors should be taken into account for rack solutions. E.g. some blade server solutions can weigh up to 250kg when fully populated, which means a fully-populated rack can weigh more than 1000kg. Most raised data centre floors are not designed to carry loads this large.
- To ensure optimum use of cooling resources, blanking panels should be installed in racks with free space.

4.1.5 Data centre design

- Design or planning of data centre facilities should be done in conjunction with Department of Public Works.
- Power consumption: more and more computing environments are forced to make a trade-off between absolute performance and cooling and power supply constraints. This is certainly true of most data centres, is even becoming a concern for stand-alone servers. New technologies and methodologies are addressing this issue to an increasing extent, but as computing requirements keep increasing, power use needs to be monitored and managed carefully. Focussing on a value-per-Watt measurement may be the best way forward as data centre computing becomes more dense and power-hungry.
- Redundant cooling infrastructure should be considered for mission-critical environments. While this is more costly up-front, it will go a long way towards ensuring system availability. Despite the fact that servers and storage solutions may have redundant components, a single air conditioner failure could bring down or damage all these systems.
- Cooling and UPS sizing are directly related to the power requirements of computing and storage solutions, and these need to be factored in before deploying the data centre infrastructure.
- Due to the size and design of some solutions, physical data centre constraints must be taken into account:
  - Floor load carrying capacity (e.g. 250kg mass per 10u blade chassis)
  - Electrical capacity (total amperage)
  - Electrical connections available
  - Cooling capacity (BTU capacity)
  - Accessibility (delivery/loading zones, doorway dimensions, elevators, stairs, etc.)
- Large data centres should be configured in a hot aisle/cold aisle configuration to ensure optimum distribution of cool air.

4.1.6 Solution certification

- Compatibility and vendor certification (in addition to the basic Servers and Storage specifications) should be made prerequisites in any RFP/RFQ. While base compatibility with industry standards is catered for by the detail specification, any unique or specialised requirements must to be addressed by the supplier proposal (in conjunction with SITA if required).
- The reliability of a solution is often directly related to system complexity. Environmental factors such as data centre design, network and electricity reticulation also play a significant role. In addition, the reliability of individual components affect system availability. For highly-available solutions, redundancy and other RAS requirements must be specified up front.
- After completing the installation of an Servers and Storage solution, suppliers are required to formally commission the solution, with formal acceptance of a working solution by the client. Clients can request audits where exceptions are raised about functionality: in case of a dispute or complaint, SITA can be involved to verify whether the solution fulfils stated requirements.

4.2 Supplier guidelines (normative)

Where applicable, certified suppliers are required to adhere to the following normative standards when supplying products certified via the Servers and Storage domain:

- 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 Servers and Storage 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.
- As part of the SLA, warranties for the individual components that make up the solution (e.g. servers, switches) must be managed by the supplier on behalf of the client.
- Support contact details (call centre) must be provided to the client at delivery/commissioning.

4.3 OEM responsibilities (normative)

SITA has concluded an MoA (Memorandum of Agreement) with more than 120 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.

4.4 RFP/RFQ process

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

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

- Ensure that all applicable guidelines in this Deployment Guide are followed.
- Determine and **document detail requirements** (see guidelines and requirements sections for specific information around this).
- Verify **appropriate sizing** of requirement before publication.
- Approach SITA for **advice** (if required).
- A bill of materials may **not** be specified, as this places the burden of a working solution on Departments, instead of bidders.
- Domain Item names (e.g. PC3, MF4, Srv1) 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, advanced displays or

extra storage), services such as regional delivery, installation and maintenance, or upgrades from the base specification to meet additional performance requirements.

- **Publish request** with documented requirement. All information about requirements, infrastructure, constraints, etc. must be shared with all respondents, i.e. if new information becomes available during adjudication, all respondents must be allowed to update their responses. Any requirement not stipulated up front may not be used to adjudicate bid.
- Suppliers may only quote solution components, equipment, accessories and upgrades that were listed in the product detail specification at certification. This is to ensure that the solution is made up only of certified components.
- Evaluate RFQ in terms of TCO, BEE and compliance with requirements (technical). The **PPPFA 90/10 principle** must be utilised in this process. Departments are encouraged to tailor TCO calculations for their specific environment. It is important to verify during the technical evaluation that **all mandatory components** (e.g. 3-year support) are included in the quoted price, using the submitted bill of materials or pricelist. This is to ensure a fair, apples-to-apples cost comparison.
- Award to the most **suitable bidder**, i.e. the one with the highest-scoring bid that complies with all requirements.

The Engagement Model has more details on this process.

4.5 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 in the province where the solution must be delivered/installed.
  - Certified to supply the required product Category and Item.

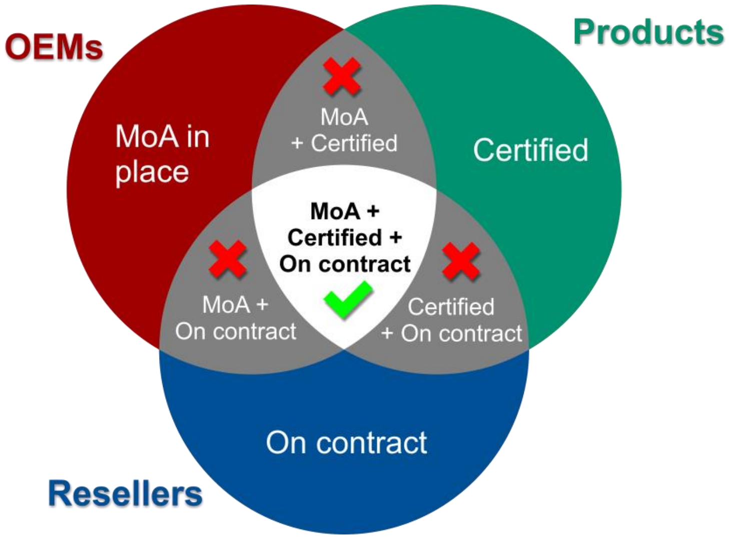


Figure 6: Requirements for supply to Government

- 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).
- 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.
- According to best practice, and to decrease TCO, solutions must be sourced from a single supplier, not multiple suppliers, to ensure interoperability and eliminate finger-pointing. It is not recommended to split a solution among multiple suppliers.

5. Services, best practice and deployment guidelines

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

5.1 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 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.

5.3 Service and support

- Service and support requirements must be addressed thoroughly by the client via service level agreements (SLAs). For more complex or mission-critical solutions, upgraded SLAs must be specified and negotiated as part of the procurement process.
- Detailed support and maintenance requirements must be stipulated up front as part of the specification.
- Up-to-date certification of service providers is vital to maintain OEM warranties: technician certification for some OEM products have to be renewed annually.
- Most OEMs commit to supporting a product for at least 3-5 years after being discontinued. Government can partly address this concern by opting for a more comprehensive SLA up front.
- Countrywide delivery is included as a mandatory component in all technology domains. Required delivery times must be negotiated with the supplier, and non-performance can be managed by involving the appropriate SITA resources. Delivery and/or installation of complex solutions or systems must be project-managed in conjunction with the supplier or solution architect.
- Changes to any ICT infrastructure (e.g. network or server configuration) should only be done by certified resources, whether internal or contracted. This will ensure that all changes are done in a controlled way, and system reliability is maintained.
- To ensure maximum reliability, integration and functionality, Departments are urged to procure solutions from a single supplier or consortium instead of buying different components from different suppliers. A single point of contact (call centre) must be established at the supplier for all maintenance and support. This principle becomes even more vital for mission-critical installations such as data centres.
- Maintenance for existing Servers and Storage infrastructure must be quoted as part of a full solution proposal including upgrades of the existing infrastructure. The new supplier takes on the maintenance of legacy units as part of the full solution offered.

5.4 Best practices

- Certification of products to be interoperable with third-party solutions (e.g. a VC endpoint certified by a UC 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".
- From a security perspective, installations must be hardened and optimised beyond the standard installation. Government requirements as documented in the MISS must also be followed.
- Additional installation services are available to complement proposed solutions. 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.
- OEM warranties usually exclude accidental or user damage (e.g. running a server beyond its rated temperature for an extended period). 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 fleet management solutions or hardware tracking technology.
- Suppliers 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.
- Detail planning and project management of the complete roll-out is vital to ensure control over timescales, budget and a quality installation.
- Checks and sign-offs must be done before continuing with subsequent phases.
- Just-in-time procurement of equipment is preferable (lengthy installations sometimes cause equipment to be out of date at installation time).
- The order of installation is important: changes to the facility (cabling, flooring, access control, etc.) must be done before Servers and Storage equipment is installed.

6. Conclusion

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

A thorough analysis of user requirements **must** be done to ensure that a fit-to-purpose solution is procured. In general, a solution specification should be stated in plain English, focussing mostly on business requirements, avoiding unnecessary detail technical specifications. SITA can assist Government in the requirements analysis process 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 Customer Relationship Managers).

Lastly, many individuals and organisations have contributed to this document, and TAS will keep updating it with useful information and guidelines. 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
Izak de Villiers	Technology management and consultation	izak.devilliers@sita.co.za 012 482 2749
TAS service desk	Coordination, communication and administration	tas@sita.co.za 012 482 2872

Annex A: Sample RFP/RFQ Clauses

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

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

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

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

MANDATORY	Comply	Do not comply
Bidder must be certified by SITA as a supplier approved on the relevant transversal contract (e.g. Contract 2013).		
Substantiate: Attach proof that bidder is approved by SITA for this contract.		

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

MANDATORY	Comply	Do not comply
Bidder is certified by SITA to supply the proposed product brand(s), Category (e.g. Servers or Racks), Item (e.g. Srv1) and specific product offered in the proposal/quotation.		

Substantiate: Attach proof that bidder is approved by SITA for this Brand, Category and Item.

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

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

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

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

MANDATORY	Comply	Do not comply
Design, project plan and 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:		

PRICING SCHEDULE

To ensure compliance with all solution requirements, the various components of the solution must be itemised and priced separately, as per example:

Major solution components	Quantity	Unit Price (Excl VAT)	Nett Price (Excl VAT)
Compute component (servers)			
Storage component (disk arrays)			
Connectivity component (switches, cables)			
Software component (OS, hypervisor, management)			
Support and maintenance (SLA as specified)			
		Subtotal	
		VAT 14%	
		Total VAT Incl.	

Annex B: Technology Domain Details and Technical Specifications

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

Bundled and Optional Accessories

Since the scope of transversal Servers and Storage solutions is so wide, it is impractical for this Guide to list all possible combinations or address or possible scenarios. Therefore, a general list of accessories that **must** be delivered as part of any Servers and Storage solution is provided instead. Any additional accessories, services or components must be addressed in the RFP/RFQ, and included in the solution design 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. fabric switches in a storage solution)
- All interfaces required by the specified solution
- Remote management interface (if applicable)
- Batteries (if applicable)
- Any software application or driver required for proper functioning of the system or a component
- Rails or rackmounts kits for rack-installed systems
- Standard warranty and SLA as specified
- Proper design and planning of the solution
- Delivery and installation
- Commissioning
- Basic introductory training on the system

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

- Operating systems and hypervisors
- 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 (e.g. software, applications). Any software apart from OS and drivers are typically excluded, apart from software procured as part of the full solution (e.g. VMWare, backup software).
- Integration services (connect to existing UPS, storage, network).
- Configuration of system and/or applications (creating user accounts, shares, etc.)

- Any other component, accessory, upgrade or service not specified in the AVCT Technical Specifications at www.sita.co.za/prodcert.htm.

Annex C: Abbreviations, Terms and Definitions

Abbreviations

BEE	Black Economic Empowerment as defined by Act 5 of 2000.
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
DVD	Digital Versatile Disc
GITOC	Government IT Officers Council
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
HBA	Host Bus Adapter
HTML	Hypertext Markup Language
IpvX	Internet Protocol version (e.g. IPv6)
ISO	International Standards Organisation
ISV	Independent Software Vendor
ICT	Information and Communications Technology
IT	Information Technology
IPMI	Intelligent Platform Management Interface
JBOD	Just a Bunch of Disks
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
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 of components are acceptable
NAS	Network-Attached Storage
NAT	Network Address Translation
NIPP	National Industrial Participation Programme
NIST	National Institute of Standards and Technology
NT	National Treasury
ODF	Open Document Format
OEM	Original Equipment Manufacturer
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

PDU	Power Distribution Unit
PFMA	Public Finance Management Act
PPPFA	Preferential Procurement Policy Framework Act
QoS	Quality of Service
RAM	Random-Access Memory
RAS	Reliability, Availability and Serviceability
RFC	Request for Comment
RFQ/P/B	Request for Quotation/Proposal/Bid
RISC	Reduced Instruction Set Computer
ROE	Rate of Exchange
RSA	Republic of South Africa
SABS	South African Bureau of Standards
SACSA	South African Communications Security Agency
SAN	Storage Area Network
SCM	Supply Chain Management
SCProc	GITOC Standing Committee on Procurement
SITA	State Information Technology Agency
SLA	Service Level Agreement
SMME	Small, Medium and Micro Enterprise as defined and interpreted by Act 102 of 1996.
SNMP	Simple Network Management Protocol
SSA	State Security Agency
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
TCP/IP	Transmission Control Protocol/Internet Protocol
TTT	Technical Task Team, a sub-committee of the GITOC SCProc.
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VAT	Value Added Tax
VDI	Virtual Desktop Infrastructure
WAN	Wide Area Network
WiFi	Wireless LAN (IEEE 802.11)
WLAN	Wireless LAN (IEEE 802.11)
X64	Standard Intel-based processor architecture

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.

Term	Definition
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).
Category	A collection of technology Items (products) representing a functional area, such as Servers, Storage, Racks, 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, assemble, configure, plug into power and network, integrate into rack/server room 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. Srv2, Lib1. A product must be offered at Item level. Multiple products may be offered for each Item. Items are organised into Categories, e.g. Blade Servers, Secondary Storage, 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).

Term	Definition
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.
Repair	Any action taken by the OEM or service partner to ensure that a working solution is available to the client within the specified turnaround time. This can include physically repairing the system on-site, or swopping out the system or a faulty component.
Required	What the Client needs as a complete, working solution. Due to the transversal nature of the technical specification, detailed requirements cannot be addressed fully, but must be defined based on end-user requirements on a per-project basis.
Service zones	Geographical areas within South Africa where product and service delivery are required. These areas are designated as Zone A, B or C, depending on proximity to large centres. The zones are defined as follows, along with the required business-hours SLA: Zone A - **8-hour repair**: The entire Gauteng Province, as well as in or within 50km from major cities or Provincial capitals, i.e. Cape Town, Port Elizabeth, East London, Bisho, Bloemfontein, Durban, Mmabatho, Polokwane, Kimberley, Pietermaritzburg, Ulundi, Witbank and Nelspruit. Zone B - **16-hour repair**: In or within 50km from major towns, i.e. Welkom, Umtata, George, Grahamstown, Thohoyandou, Rustenburg, Klerksdorp, Ermelo, Standerton, Ladysmith, Oudtshoorn, Richards Bay, Saldanha, Upington, Worcester, Potchefstroom and Beaufort West. Zone C - **24-hour repair**: All towns and rural areas not included in Zone A and Zone B where services may be required. Zone C includes the entire country not covered by Zone A or B. Examples of exclusions to the on-site service requirement include equipment deployed or used on ships or other vehicles, and areas outside the immediate borders the RSA.
Supplier	Final value-added step in the channel before the end user. Compare with Solution provider
"Support for"	A capability that a product must enable, but must not necessarily have built-in or included in the base configuration without an optional accessory or upgrade.
Tech Update	Periodical refresh of technical specifications during as Government requirements change.
Technical support	A technical service rendered for out-of-warranty work, or work related to, but not covered by, the services specified as included with offered products.
Technology management	A process by which the technology specification is updated, upgraded or "refreshed" to reflect industry advancement or changes in user requirements over a period of time. The process is managed by SITA in conjunction with clients, OEMs and other role players.

Term	Definition
Transversal Contract	A term or period contract established for more than one Government department or public body, with one or more approved suppliers for the supply of information technology goods or services over a period, required. The purpose of a transversal Contract generally can be stated as addressing 80–90% of Government requirements, reducing the need for *ad hoc* tenders. Transversal Contracts exclude niche or special requirements by definition, and there will consequently always be a need for some *ad hoc* Contracts.
Upgrades	Components or subcomponents that have the purpose of expanding the capacity of the offered product, including RAM, hard disks, CPUs, etc. Upgrades are typically expansions that can be done inside the system chassis (e.g. printer duplexer or additional RAM). “Fork-lift” replacements of systems are not seen as upgrades. Upgrades are not necessarily after-market operations. A base system may be upgraded with additional capacity at purchase time.
Warranty and support	As per detail technical specifications, the following SLA conditions apply to the Servers and Storage domain: Standard warranty and support included with all supplied systems and products (as defined and qualified per technology category/Item): Countrywide on-site with full coverage (parts and labour for entire Item, upgrades and accessories) during office hours (7:30 - 17:00), with next business-day **repair** (according to Zone definitions) for **5 years** (60 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.