SITA

Deployment Guidelines:
Surveillance and Access Control (SAC) Solutions

Version: 2.0

Date: 2024-03-13

Notice

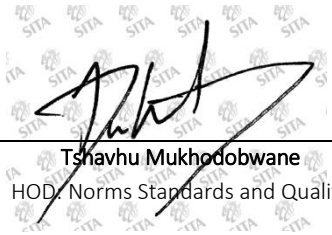
Document enquiries may be directed to:

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: Surveillance and Access Control Solutions
Document No: **eNSQS-00269**
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 defines a best practices guideline for Surveillance and Access Control solutions (SAC). It incorporates solution specification and selection guides, enabling cost-effective procurement and deployment of ICT by Government and SITA. The goal is to empower Government to procure and deploy appropriate technology solutions to meet its physical security and surveillance requirements. The Deployment Guide informs the ICT architecture of Government departments in terms of usage models, hardware, software and infrastructure requirements. It supports any procurement vehicle for physical security solutions (e.g. SITA Contract RFA 2306-2020). Complete, turnkey solutions are in view, including all required components, systems, infrastructure and associated services (e.g. installation, training, support and maintenance).

Contents

Tables

Figures

1. Introduction and background

This Deployment Guide recommends best practices for specifying and deploying solutions from the Surveillance and Access Control technology domain (comprising fixed and mobile cameras, video recorders, networking equipment, video management and monitoring systems, access control technologies, and related physical infrastructure), 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 intended to complement Departmental ICT policies and processes, 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.

Specific business requirements are not addressed in this document, and must be documented on a project basis, with input from TAS where required. **Requirements and Sign-off Checklists** are available for download to help project managers capture client requirements and manage solution roll-outs. Examples of these are available in Annexes A and B. **RFQ/RFP questions** and a **Pricing schedule** are included in Annex C, to be incorporated into Requests for Quotation/Proposal. Using these aids, Government should be able to combine systems, services, connectivity and functionality across all domain categories to procure unified surveillance and/or access control solutions.

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.

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
- SITA contract RFA 2306-2020 for Surveillance and Access Control Systems:
  - Engagement Model: RFA 2306-2020
- Processes and standards:
  - 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

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:

- **Open industry standards (*de jure*):** These include standards such as those published by the IEEE, IETF and ISO/IEC, e.g. TCP/IP, Wi-Fi, HTML, ONVIF, 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 conform to them to meet interoperability requirements. Operating systems such as Google's Android may be included here. Like open standards, these standards also enable interoperability, but more by virtue of their wide deployment than formal standardisation. Other examples of *de facto* standards are Windows in the desktop space, or Dante in the AV domain.

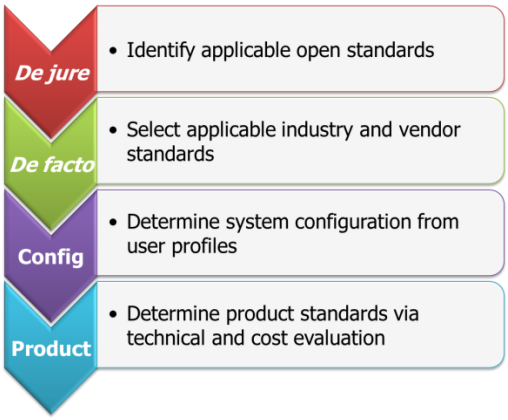


Figure 1: Standards selection process

- **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 devices uniformly to reduce effort and costs associated with system deployment and management.
- **Product standards:** Configuration standards can be applied to select 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 where Departments move from *de* jure standards through *de facto* and configuration to arrive at product standards that meet their 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

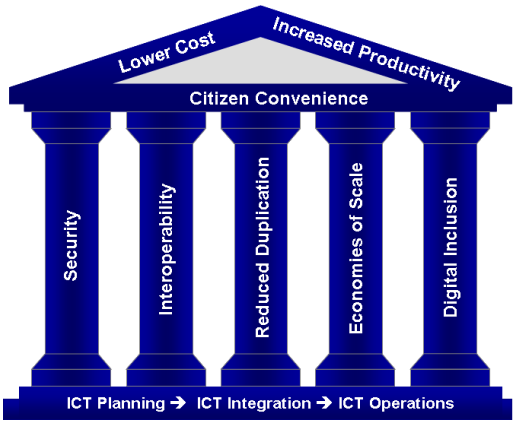


Figure 2: ICT House of Value

- 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
- 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 the Technology Task Team (TTT)
- 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 Surveillance and Access Control solutions
  - 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 DCDT, GITOC, Government stakeholders and industry, a **Technology Certification Process** (TCP) according to which specific classes of products can be certified. At the time of writing, these classes of products include the following technology domains, with the domain under discussion emphasised.

Domain	Components
Personal Computing Devices	Desktop PCs, Mobile PCs, Desktop displays, Mobile devices (Tablets, Smartphones, Industrial handhelds), Accessories and Device Management
Peripherals	Printers, Multifunction devices, Scanners, Digital cameras, Automatic Data Capture (Barcoding, Card devices), Biometric readers, Consumables and Print management
Assistive Technologies	Assistive devices and software for people with disabilities, including smart devices (tablets, PDAs, readers, media players, recorders and braille

Domain	Components
	devices), peripherals (input and output devices) , assistive software enabling access and speech (AAC), and skills development and learning aids for users with disabilities
Education Solutions	Classroom solutions, including PCs, laptops, tablets, presentation and teaching devices, Classroom infrastructure and systems (hardware and software), and e-Sports systems
Audiovisual Communications (AVC) Technologies	Video and audio conferencing, large-format display devices (projectors, monitors, interactive displays and display walls), collaboration, media recording, speech processing, and AV signal control and management
Surveillance & Access Control (SAC)	**Fixed and mobile surveillance and physical access control solutions, including IP cameras, mobile cameras, UAVs, storage and recording devices, video management systems and control room solutions**
Servers & Storage	Servers (Rack-mount, Tower, Blade), Primary storage and Secondary storage (Disk to disk, Tape automation and Archiving) and System management
Networking	LAN, WLAN and WAN equipment, Wireless backhaul, and Structured cabling (copper and fibre-optic)
Infrastructure	UPS, Equipment Racks, Alternative power, Cable ducting, trenching and routing

Table 1: Technology domains within the TCP

The Technology Certification Process requires OEMs to register with SITA, and thereafter submit their products for certification according to the standard technology evaluation process. Products are measured against ratified 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 typically requires integrated solutions spanning multiple areas and technology domains. For example, servers may be required as part of an SAC solution for a Department. These servers must be certified according to the requirements of the Servers and Storage domain, even though the broader solution is procured via the Infrastructure 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.

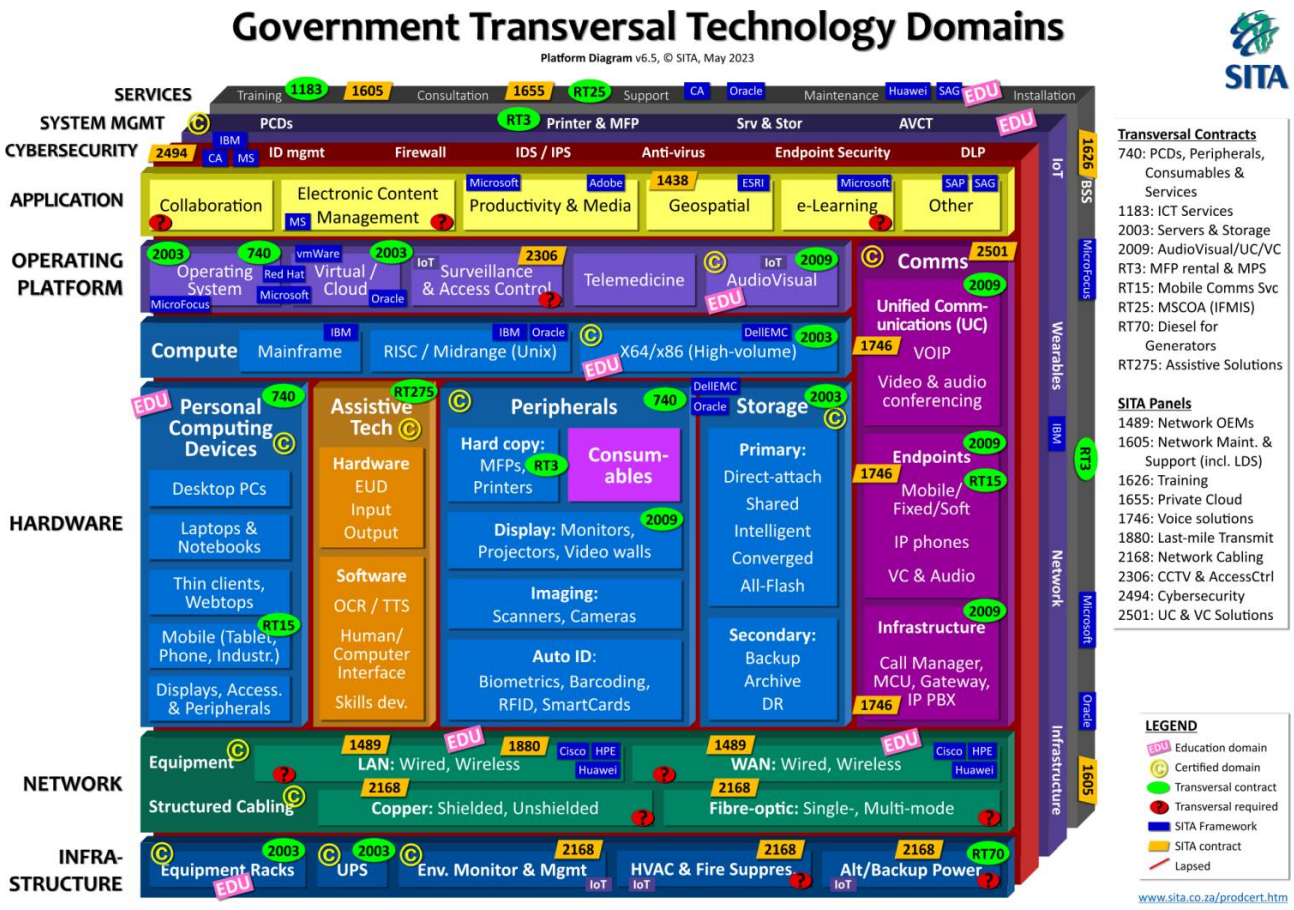


Figure 3: Transversal technology domains

The latest version of the Technology Domains 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 certification 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 and/or OEM documentation.
    b) Verify interoperability via compatibility tests and/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 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 (e.g. on an annual basis for PCD domain), 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 SAC OEMs and integrators 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 cost analyses.

Certification of new or replacement 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 Surveillance and Access Control Domain

The purpose of the technology domain is to specify and certify suitable solutions for deployment within Government, in support of any procurement vehicle established in this space (e.g. SITA Contract RFA 2306).

In order to fulfil their mandate, video surveillance solutions must record and retrieve video footage and images of sufficient quality that they can support any defined business and legal process, including evidence for criminal proceedings. If this quality requirement is not met, the money spent on the solution is effectively wasted.

The same applies to other categories within the domain, such as access control solutions: effective physical access control and safety must be established and maintained by any system deployed in terms of the SITA process.

If any deployed SAC solution does not meet minimum business and operational requirements, it will have to be repaired, upgraded or replaced, resulting in double expenditure to Government. To prevent such fruitless expenditure, SITA has established technical and deployment standards that are captured in this and other related documents.

2.1 Scope

The Surveillance and Access Control technology domain comprises the following categories and technology types, which inform the building blocks to be used to design and deliver SAC solutions:

Category	Technologies
Video Surveillance Solutions	Fixed surveillance (IP camera systems), Mobile

Category	Technologies
	surveillance (vehicle/wearable cameras and sensors), Surveillance Infrastructure
Access Control Solutions	Access readers, controllers and software systems
IoT Solutions	Mobile and fixed sensors
Physical Safety Solutions	Alarm, Public Address and Evacuation Systems
Additional solution components (non-ICT)	Essential solution components that are not ICT-based, including infrastructure
Services: Bundled and *Ad Hoc*	Essential services, both mandatory and optional, including training, support and maintenance and consultation

Table 2: Categories in the SAC domain

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

Note: The certification process for the SAC domain does not cover non-ICT components, but solutions incorporating these must adhere to the guidelines and standards defined in this Deployment Guide.

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, 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 determined by client and business requirements, and therefore an RFP/RFQ process must be used to define client needs on an *ad hoc* or project basis. To ensure the lowest possible TCO, the following elements are specified and/or measured during evaluation:
  - Usage profiles based on business requirements
  - Reliability, availability and serviceability (RAS) of the solution
  - Comprehensive countrywide on-site SLA with upliftment options
  - Manageability: Remote management, automated failure alerts, remote diagnostics and updates
  - Duty cycles and data volumes in terms of usage profiles
  - Environmental factors such as power quality, energy consumption and cooling requirements
  - Other elements impacting productivity, including quality and usability
- Service levels:
  - Comprehensive 5-year on-site warranty and next-business-day repair SLA
  - Supplier training and certification by OEM
  - Improving supplier service and quality via OEM process
  - Dispute resolution between Government and industry
- Performance and functionality: by leveraging technology architectures, the best possible solution can be ensured for Government applications
  - System architecture and functionality
  - Connectivity capabilities and options

- Upgrade options and accessories
- Security (e.g. physical access control, surveillance , secure system management)
- OEM-level certification according to quality and environmental standards
- Product-level certification according to national 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 Surveillance and Access Control domain supports the acquisition of **complete, turnkey solutions**, including any related component, infrastructure or software-based system that may be required by Government. Associated services, components, accessories, services by OEM partners, 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 all that is necessary (e.g. purchasing a few cameras or upgrading storage), but more often clients require a fully functional turnkey solution such as an entire surveillance and security solution, including access control and monitoring, with all services, technologies and infrastructure components fully integrated.

Figure 4 illustrates the relationship between domain components or products and the services rendered by suppliers to arrive at a full solution that meets 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.

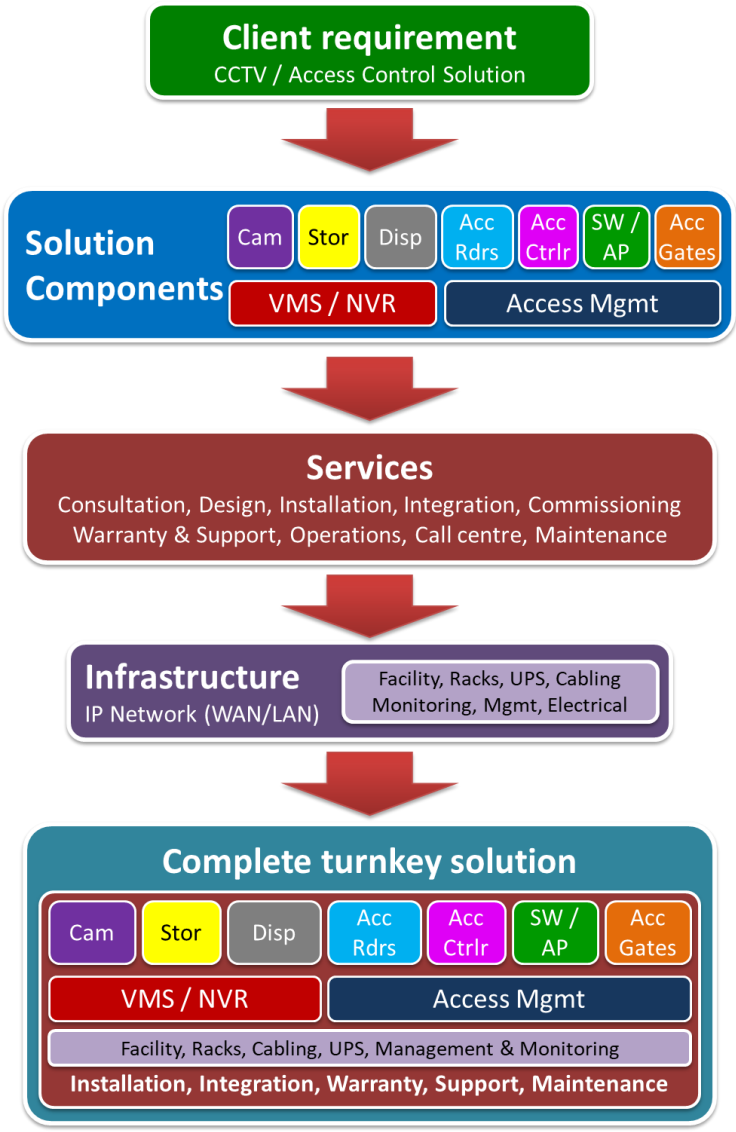


Figure 4: Turnkey SAC solution

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.

Figure 5 illustrates the relationships between the major phases of a SAC project. Business and solution requirements are central, and must be prioritised at all time.

Figure 5: Business requirements

2.4 Domain components and usage profiles

The components of the SAC 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 SAC 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 Surveillance and Access Control Solutions

The intention of this technology domain is to combine devices, services, connectivity and infrastructure across all relevant categories to establish a unified video surveillance system (VSS).

Fixed surveillance (IP cameras)

Item	Description	Usage profile
Cam_IP1	Indoor IP camera	IP camera range for indoor use; various form factor, resolution and lens options
Cam_IP2	Outdoor IP camera	IP camera range for outdoor use; various form factor, resolution and lens options
Cam_IP3	PTZ IP camera	IP camera range with pan/tilt/zoom functionality; various form factor, resolution and focal length options
Cam_IP4	Thermal IP camera	IP camera range for thermal applications; various form factor, resolution and lens options
Cam_IP5	Specialised IP camera	IP camera range for specialised applications; panoramic, multi-sensor, modular/discreet, distributed sensor, or other advanced/special capabilities

Table 3: IP camera profiles

Mobile surveillance (mobile/wearable cameras and sensors)

Item	Description	Usage profile
Cam_Body1	Basic body camera	Basic body-worn camera with wireless LAN, lightweight, robust design and integrated mounting hardware
Cam_Body2	Advanced body camera	Advanced body-worn camera with wireless WAN connectivity
Cam_Vehicle1	Basic vehicle camera	Basic vehicle camera
Cam_Vehicle2	Advanced vehicle camera	Advanced vehicle camera with WWAN connectivity
Cam_UAV1	Basic camera UAV	Basic UAV/RPAS (drone) with integrated camera
Cam_UAV2	Advanced camera UAV	Advanced UAV/RPAS (drone) with discrete payload options

Table 4: Mobile camera profiles

Video Surveillance Infrastructure

Item	Description	Usage profile
NVR1	Basic NVR	Network video recorder range with basic functionality and capacity
NVR2	Midrange NVR	Network video recorder range with midrange functionality and capacity
NVR3	Advanced NVR	Network video recorder range with advanced functionality and capacity
VMS1	Basic video management system	Video management system with basic functionality and capacity
VMS2	Advanced video management system	Video management system with advanced functionality and capacity, including analytics options
Stor_VS1	Basic video surveillance storage	Basic storage system for surveillance footage
Stor_VS2	Advanced video surveillance storage	Advanced storage system for surveillance footage

Table 5: Surveillance infrastructure profiles

2.4.2 Physical Access Control Solutions

Item	Description	Usage profile
Acc_Reader1	Access reader: PIN/card/token	Access control reader with keypad and/or support for various access tokens (card/proximity tag/mobile credential)
Acc_Reader2	Biometric reader: fingerprint	Access control reader supporting fingerprint biometrics
Acc_Reader3	Biometric reader: face	Access control reader supporting face biometrics
Acc_Reader4	Biometric reader: touchless	Access control reader supporting touchless biometrics (fingerprint, palm, palm vein, iris etc.)
Acc_Ctrlr	Controller for door/gate access	Single- or multi-entrance access controller
Acc_Mgmt	Access control management system	Central management system for access control solutions and components, including controllers, readers, doors and users

Table 6: Physical access control profiles

2.4.3 Additional SAC components (non-ICT)

Non-ICT AV products and components (requirements defined in *ad hoc* RFQ/RFP)

Description
Gates, turnstiles, booms, vehicle barriers
Lighting (visible + IR)
Analogue alarm systems
Sensors (beam, IR, radar, etc.)
X-ray scanners
Metal Detectors (Portal + Handheld)

Description
Civil works: trenching, etc.

Table 7: Physical access control profiles

2.4.4 Services: Bundled and *Ad Hoc*

Services that may be rendered as part of an SAC solution include, but are not limited to, the following:

- Consultation (including development of the operational requirement as per SANS 10222-5-1-4)
- Design (solution design, including camera placement according to SANS 10222 OR)
- Specification (including camera position, type, lens, viewing distances, IR requirements)
- Supply and delivery
- Installation
- Integration
- Commissioning
- Training
  - Generic SAC principles and concepts (including image quality evaluation)
  - Solution-specific training
  - PSIRA training
- Support
- Operations and Maintenance (including regular quality and performance audits)
- System management
- On-site technical resource
- End-of-life services

The following requirements apply to all supplied services:

- All services to be quoted and supplied as required by project needs.
- Basic services such as delivery, installation and support must be bundled with ALL solutions, as per the Detail Specification.
- The standard 5-year SLA can be upgraded further at the client's discretion.
- Specialised or ad hoc services will be specified in the client RFP/RFQ, and must be fully catered for by the proposed solution.
- All required travelling and accommodation (S&T) must be included in the quoted total solution cost.

2.4.5 Other components and services

In addition to the above devices and services, the following infrastructure may be required as part of a complete solution:

- Ducting, trenching and routing for cabling infrastructure
- Backup power, surge protection and other power requirements (including electrical work)
- Civil construction work, including structural modifications (if required at the site/facility)

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 SNMP, DNS, DHCP, IPv4 and IPv6.
- Holistic systems management, allowing support staff to remotely monitor, configure, update and troubleshoot systems and devices, saving on labour and travelling costs, and minimising downtime.
- Countrywide, **5-year on-site warranty** with next-business-day **repair** SLA for all systems (Zone A only; Zones B and C extend the repair time to 2 and 3 days respectively). To further ensure maximum productivity, SLA upgrade options are also mandated for all products, which can be procured at the client's discretion. This warranty and SLA must be included in the up-front payment at project acceptance in order to lock in the warranty and maintenance contract with service providers, and ensure competitiveness and the lowest possible TCO.
- 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.
- Software licences for all basic functionality as specified are included in the Base Price. Additional software functionality 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 additional cost to the user.

2.6 Bundled accessories and services

Both the technical specification and this Guide prohibit suppliers from quoting or delivering incomplete solutions.

Each SAC solution must be specified as a **fully working, turnkey system** with a minimum set of mandatory bundled accessories and services. For example, all solutions must be bundled with the minimum SITA-specified configuration, including, e.g. standard SLA, software, 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 different lens or reader configuration.) 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 requirements such as upgrading the standard support SLA.

All solutions must be bundled with the standard specified **on-site support SLA** included in the quoted price. To ensure the lowest possible TCO for Government, the warranty and support **may not** be unbundled from the total price.

The SITA 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.

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. 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. Surveillance and Access Control guidelines

Deploying a surveillance or access control system does not automatically result in a secure physical environment: these systems are tools that still require effective security people and processes to administer them and act on alarms or other information generated by the system.

Video surveillance solutions have three main purposes:

- Deterrence (through visible elements such as cameras and quick-response measures)
- Live monitoring (e.g. perimeter monitoring or licence plate recognition)
- Support of investigations after an incident occurs (including identification of persons)

These three goals all rely on an effective, correctly-implemented system to achieve the client's stated surveillance requirements.

Automated AI-driven video analytics systems can help to ease the burden of surveillance operators and increase the overall effectiveness of the system. However, like human operators, these technologies also have limitations that need to be recognised and planned for.

Surveillance and access control solutions extend much further than just purchasing cameras or card readers. If these devices are not coupled with the required support systems, infrastructure and services to achieve a complete, integrated turnkey solution, any money spent will effectively be wasted.

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

3.1 Business requirement

The most important principle in deploying any ICT-based system, including surveillance and access control solutions, is that the **end-user requirement** must determine the type of system or solution 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 security system serving a specific building or campus).

Once the basic business requirement is met, secondary considerations such as additional functionality, cost, manageability, 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 processes or business functions.

3.2 General principles

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

- The end-user surveillance needs must be used to determine the quality of images and video required (e.g. monitor, detect or identify). All other system elements and capabilities must be derived from this information. If forensic-quality video is required, the cameras, network, storage, video management system and processes must support this goal. Note that display quality, video frame rate and resolution will influence network utilisation, latency, and hence the monitoring experience and effectiveness.
- 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.
- Cost-effectiveness: value for money for every SAC solution implemented in Government. This includes ensuring long-term service and support, product quality, security and functionality. If the resulting SAC solution does not meet the business requirement, this will effectively result in fruitless expenditure. Article 217 of the SA Constitution requires cost-effectiveness, which effectively excludes cheap, sub-standard products or solutions, requiring solutions to be both financially affordable and technically capable. Therefore, cost-effectiveness can only be achieved if a high-quality, fully functional, 100% compliant solution is procured.
- Detail product specifications (e.g. sensor resolution, exact product dimensions and weight) should not be used to define an end-user requirement. The business need must be defined based on actual operational needs.
- The SAC technology 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 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 installation, commissioning, 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.
- Expandability and upgradeability must be planned for to ensure the longer-term usefulness of the SAC system. This includes upgrading storage capacity, control room capabilities, camera functionality, back-end system throughput, etc.

3.3 Security

The security architecture of any ICT system is a vital component of the total solution. Standards are in place to address minimum security requirements, but practical measures also need to be taken (e.g. logical access control) at system and individual device level.

SAC systems and access control devices must be secured (hardened) according to OEM and industry best practices during implementation. All relevant security information (e.g. passwords) and steps to be followed must be handed over to the client after commissioning, at acceptance of the solution.

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

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

- Do not connect any surveillance or access control systems directly to the Internet.
- Enforce logical access control (user authentication) for all systems and networks.

- Set and enforce a strong password policy for users and administrators – under no circumstances must the default password for any device be left in place.
- Disable unused user accounts (e.g. Guest user).
- Only open TCP ports that are specifically needed by the system, and disable unused or outdated ports and protocols (e.g. FTP, Telnet).
- Set secure passwords for all remotely accessed devices and services.
- Disable management/media ports if they are not used.
- Disable all unused services/daemons on the device.
- Ensure that firmware and software are updated regularly to address vulnerabilities found by the OEM in the interim.
- As far as possible, use the latest versions of protocols (e.g. SNMP v3) to avoid vulnerabilities in the older versions.
- Use secure versions of protocols where possible (e.g. HTTPS, SSH, SNTP) – these use encryption to secure communications via the network.
- Monitor and manage devices using a standard, secure management tool.
- Change or disable settings that are insecure by default (e.g. default password, SNMP "public" community string).
- Follow the principle of "least privilege", by providing users with only the access needed to perform their specific task. All surveillance and access systems allow multiple levels of user privilege, and these should be leveraged. No system should allow public access where anybody with a network login can login to a surveillance system or device to make changes.
- Restrict physical access to the system: if a malicious actor gains physical access to a device or service, there is no limit to what damage can be done via the network.
- Where possible, encrypt device and system storage to prevent unauthorised access.
- Enable audit trail on the system to keep a log that records changes made, when and by whom.
- Use a VPN when accessing any system or device remotely.
- For access control systems, ensure that secure protocols are configured where possible: OSDP has replaced the traditional Wiegand standard, allowing greater flexibility in installation, but also enabling encryption of communications between controllers and readers.

3.4 Physical environment

It is estimated that more than 90% of surveillance video image quality issues arise from insufficient or inappropriate lighting. The placement of cameras must take into account best and worst lighting conditions (including indoor/outdoor, day/night cycle and seasonal changes) and plan for the worst case to ensure adequate coverage.

The height above ground that a camera is mounted at has a significant impact on the usefulness of the footage that is captured. If too high, facial images may not be visible, while cameras mounted too low may face light interference from ground-level sources (e.g. vehicle lights) or even the sun. It may even be possible that solar radiation can permanently damage camera sensors. A good guideline is for to pole-mounted external cameras to be at least 3m above ground to avoid vandalism while providing adequate coverage.

3.5 Infrastructure

- A software-based system such as a VMS will need IT infrastructure to support it: this must be specified as part of the complete solution, taking into account the compute and storage requirements of the system itself. For example, a software-based video management system (VMS) will require a computer and operating system on which it can be loaded and run, and storage on which to save surveillance video. IT infrastructure can include elements such as servers, operating systems, storage, connectivity and other related hardware.
- Providing a high-quality electricity supply is a major requirement for SAC installations, ensuring reliability, service continuity and maintenance of physical security, and also minimising risk of equipment failures due to poor power quality: UPS as well as alternative backup power (e.g. solar or generator) are mandatory to maintain service during power outages.
- Cabling is a vital component of any SAC solution: SITA-certified cabling systems of the correct design and performance are required to ensure optimal operation. PoE is a major contributor to highlighting cabling faults and deficiencies – especially given that many SAC endpoints (e.g. IP cameras) are powered via the network. Deploying SITA-certified cabling solutions will ensure that the correct type and quality of cable is available, conforming to international standards and best practices. Note that **CCA** (copper-clad aluminium) cable must **not** be used, since it is does not conform to mandatory standards, and does not provide the necessary infrastructure for powered or high-bandwidth solutions.
- Where applicable or required by data transmission needs (specifically for video) a dedicated network must be made available for SAC solutions to ensure that the video system does not negatively affect the rest of the environment, and vice versa. This may take the form of dedicated access-layer switches to connect only cameras for each specific wing in a building, for example. The network design must be informed by the e.g. envisioned bandwidth requirements, camera numbers, as well as integrated needed into the broader network.

3.6 Video surveillance implementation

The implementation of surveillance solutions is guided by SANS 10222, which provides a process and guidelines for measurement of solution conformance and performance. According to SANS 10222, there are 4 primary criteria for video surveillance, each with a corresponding image quality requirement in terms of historical surveillance deployments:

Identify	Image ≥ 120 % of screen height
Recognise	Image ≥ 50 % and < 120 % of screen height
Detect	Image ≥ 10 % and < 50 % of screen height
Monitor	Image ≥ 5 % and < 10 % of screen height

Table 8: SANS 10222 image quality criteria

In addition to these guidelines, the standard states that viewing angles and lighting must suit the stated requirements, and image quality-degrading factors, such as motion blur or poor focus, must be eliminated. This must be done by proper design and implementation of the solution.

Given the somewhat outdated guidance from SANS 10222 (based on the screen height of a CRT monitor), the industry has produced updated guidelines in terms of discrete pixels allocated to an object for each surveillance quality level:

Detect	Unidentifiable object has been detected	1.5 pixels
Classify	Distinguish between inanimate (vehicle) and animate (person or animal) object	6 pixels

Recognise	Object can be distinguished as a person	12 pixels
Identify	Identity of the person is easily distinguishable	25 pixels

Table 9: Updated VSS image quality criteria – DCRI

In addition to the DCRI metric, the EN62676-4 defines different levels of detail for Detection, Observation, Recognition, and Identification (DORI) for visible light and near-IR surveillance, as well as thermal imaging cameras. Measurements are in pixels/metre.

Detail level	Description	Visible / NIR	Thermal
Detect	Determine human presence (few details visible)	25 ppm	1–3 ppm
Observe	Discern characteristic details of individual	62 ppm	-
Recognise	Verify whether the individual is known	125 ppm	3–7 ppm
Identify	Positively identify the individual	250 ppm	5-14 ppm

Table 10: Updated VSS image quality criteria – DORI

- Surveillance solutions must be designed to meet the specific application criteria in the above table in order to deliver the required level of performance.
- Cameras must be installed in strategic positions to observe all doors and entrances into the site, cover all other important internal areas or rooms, as well as the outside of site buildings.
- All camera signals must be relayed via a shared or dedicated IP network to a local Network Video Recorder, with footage and alerts being viewable from a local monitoring station. Recorded data and metadata must also be viewable from a remote control centre, and recordings must be replicated to a remote storage facility if required.
- Adherence to all identified surveillance and/or access criteria as defined in the URS must be verified during commissioning, before the project is signed off. If the criteria are not met, the project cannot be finalised until the issues have been resolved.
- A viewing and export facility must be available on each site to ensure effective monitoring and access to footage for evidence purposes. This may be as simple as a dedicated PC or software loaded on a manager's existing PC. The main operations centre should not be used for this function, as it impacts on the day-to-day operation, and could compromise overall security. In addition to these considerations, management needs access to the system without having to be present in the control room.
- All surveillance components allow image and video compression to efficiently use network bandwidth and storage resources. However, care must be taken to use this function correctly, since excessive video compression can render the footage useless.
- The system should not rely on vigilance of human operators to detect incidents and act accordingly in a timely manner. Automation should be implemented as far as possible so that operators are notified of possible events detected by the system. This saves on manpower, and increases effectiveness and accuracy. This type of system can allow operators to concentrate only points of interest or specific incidents, instead of continuously monitoring all cameras for possible incidents.
- System management: solutions must be implemented to enable exception alerts, status reports, error messages and usage statistics, depending on client requirement.

3.6.1 Camera specifications

RFPs often just specify the form factor and resolution (megapixels) of the required camera, however this is insufficient. The type of lens (e.g. field of view, fixed or vari-focal), deployment environment (e.g. indoor, outdoor) and any advanced features required (e.g. human or vehicle recognition) must be addressed in

order to achieve the desired output from the camera. The camera checklist (example in the Annex) can be used to capture all the relevant requirements details per camera.

3.7 Access control implementation

Logical or physical access control leverages the following types of identification information about the user:

- What they **know** (e.g. a PIN or password)
- What they **have** (e.g. an ID card or access token)
- What they **are** (e.g. one or more physical traits or biometrics such as fingerprints, retina pattern or facial structure)

These can be further augmented with location-based, time-based or behaviour-based metrics to make the authentication more accurate and secure.

The most basic access control system implemented in Government currently is a simple token (access card based on RFID or other technology) used by employees to gain access to their workplace or other Government facilities. In this case access is based on what the user **has**, i.e. the access card. For some environments this may not be sufficient due to enhanced security requirements, or due to the risk of access cards being borrowed, lost or stolen.

In general, an access control reader is installed in an open area, a region or zone where access is not controlled, that is open to the public. The access reader is coupled with a door, turnstile or other mechanism to restrict access to non-public zones by checking credentials and access rights of users who request access to the facility's restricted area.

Once the access control factors have been determined (e.g. use of a PIN together with an ID card and fingerprint), users must be registered and enrolled on the system in order for them to be verified/authenticated when entering the facility. The enrolment process for biometrics is a vital success factor: if done poorly, the access control system will never work effectively. Enrolment needs to be done by trained, skilled workers in an ideal environment, capturing all the necessary data to ensure viability of the biometric system over time.

3.7.1 Access control readers

An important factor in the cost and functionality of an access control system is the type of reader that will be installed. Ranging from simple, low-cost devices to advanced stand-alone biometric readers, there is a wide range of access reader products available to suit all types of requirements:

- **PIN reader:** basic and simple reader offering a low level of security.
- **Card reader:** offers a higher level of security, but cards can be stolen, borrowed or lost. Often used in conjunction with other types of reader such as fingerprint. Various types of RF-based card technologies are available, ranging from low-cost, low-security cards to high-end chip cards with built-in encryption. The reader must match the card technology that is used, and the card type must match the level of security required by the facility.
- **Mobile device:** some solutions allow storing the access token on a smartphone or smartwatch, allowing the user access to the facility without a physical access card. The smart device offers a significantly higher level of security and flexibility.
- **Biometric reader:** several different biometric modalities are available depending on the level of security, convenience and cost. These are discussed in the next section.

In addition to the type of token or biometric, the positioning and weather-proofing of a reader are important factors. Throughput/read speed is important for high-traffic entrances, where touchless readers may be preferable despite higher cost. The types of electronic door locks actuated by the system must also be taken into account, as well as alternative means to open the door in an emergency, or having the door open automatically in case of fire.

3.7.2 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 11: 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.

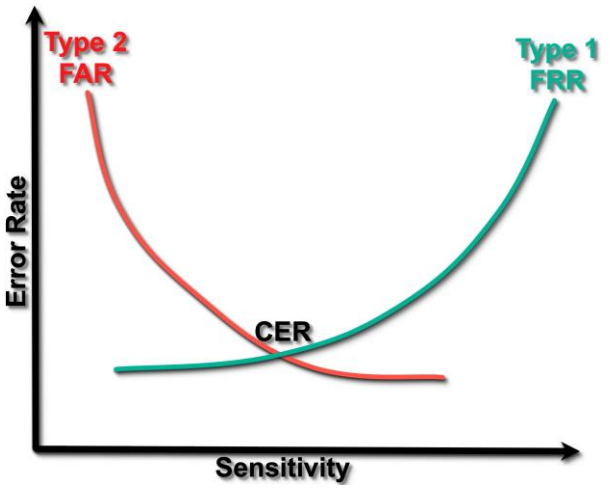


Figure 6: Biometric FRR vs. FAR

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.

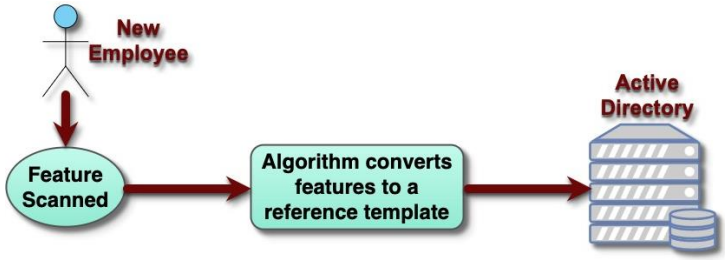


Figure 7: Biometric enrolment

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.

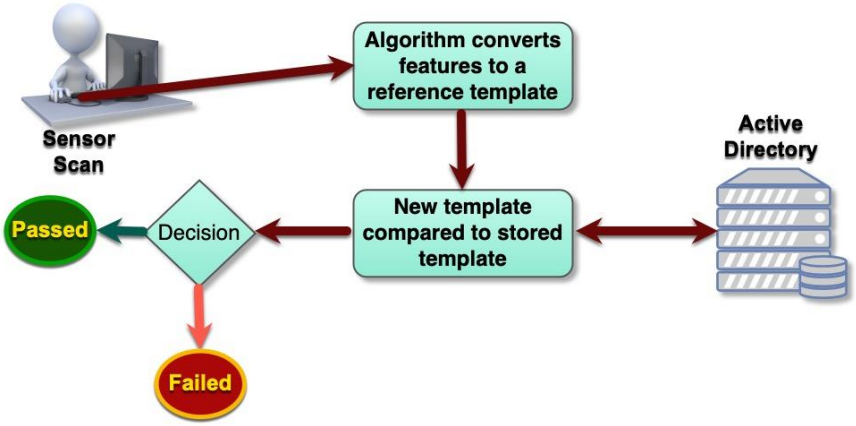


Figure 8: Biometric verification (pass/fail)

3.7.3 Requirements analysis

The following factors determine the type and complexity of the required access control system. These factors must be communicated to prospective service providers in an RFQ/RFP document.

- Integration with existing systems/environment: i.e. is this a green-fields scenario or must the system communicate with existing systems or platforms
- Upgrade of existing system or new installation
  - Existing devices to be replaced? Controllers, cards/tokens, readers.
- System capacity:
  - Number of users (current + projected growth over 5-10 years)
  - Estimated total number of transactions per day
  - Traffic level per door (e.g. front door vs. basement storeroom)
  - Peak traffic estimate: highest-volume entrance

- System architecture:
  - Local or remote access control server
  - Physical environment: number of access points/gates/doors
  - Number of doors/entrances and opening windows that must be monitored and/or controlled via alarm/access system
  - Level of security needed (general access vs. high security for sensitive areas)
  - Entrances with dual readers (entry + exit) vs. single reader + exit button
  - Types of entrances: door vs. turnstile vs. boom
- Reliability requirements: Uptime, redundancy, backup mechanisms including power
- Types of access control modalities: PIN/token/biometric/combination
  - Touchless biometric requirement?
- Specific access control requirements:
  - Anti-passback
  - Time and attendance
  - Visitor management
  - Intercom
  - Maintain occupancy levels
  - Roll call
- Specialised environment: outdoor, industrial, chemical, etc.
  - Cater for people with disabilities
- Device requirements:
  - Indoor vs. outdoor
  - Stand-alone vs. controller-based
  - UI needs: display / touch / intercom
- Supplier requirements:
  - OEM-certified and authorised to design, supply, support and maintain the solution.
  - PSIRA-accredited (expires every 12 months; must be up to date)
- Industry requirements:
  - SABS, PSIRA or any other local industry standards as applicable

3.8 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 in the RFQ/RFP 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 Surveillance and Access Control OEMs commit to supporting a product for at least 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 system (e.g. network or management 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 must procure SAC solutions from a single supplier 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 control centres.

3.9 Policies and strategies

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

- Security policies in terms of information, surveillance and physical access control
- Information management policies and strategies:
  - Data management policy (specifically surveillance video and access control data such as biometrics)
  - Storage and backup strategy, policy and procedures
  - Archival policy
  - Disaster recovery (DR) policy and strategy
- Support strategy
- Maintenance strategy

3.10 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) must be acted upon and implemented as recommended to ensure the best possible availability and reliability from the system.

3.11 Supplier responsibilities

Where applicable, certified suppliers are required to adhere to the following conditions when supplying products certified via the SAC domain:

- **The final responsibility for a working SAC 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 propose suitable and appropriate solutions as per Government's stated business requirements.
- Only SITA-certified products and solutions may be offered to Government via the SAC domain, as stipulated in the SITA Act and NT regulations.
- Suppliers must be certified by the relevant OEMs and security industry bodies to supply, install, support and maintain all the products proposed in the solution design.
- 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. UPS and racks) 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.

3.12 OEM responsibilities

SITA has concluded an MoA (Memorandum of Agreement) with more than 190 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:

- Support all their partners in terms of certification, training, solution design and regional service provision.
- Take responsibility to determine the appropriate components required to build a working solution, and communicate this to all OEM partners.
- Ensure that the optimal configuration for the stated user requirement is delivered by suppliers.
- Participate in the technology management process as per domain conditions (refer to **Technology Certification Process,** and **OEM Memorandum of Agreement**)

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

4. Procurement engagement process

The SAC domain specifies minimum requirements in terms of ICT standards, service delivery, security, connectivity, etc. Clients and suppliers are urged to familiarise themselves with these requirements in terms of their respective rights and responsibilities.

An important procurement principle is that Departments are not allowed to use specifications provided by suppliers or OEMs when publishing an RFP. The client's specific user requirement must be defined based on actual business needs. Note that any party providing support to the client in drafting specifications is barred from bidding for the solution in terms of the PFMA.

As noted earlier, the purpose of the process is to specify and implement a **turnkey solution** from a single service provider. The following basic process must be followed to achieve a successful surveillance or access control project.

SITA has established a contract (panel of service providers) from which to procure SAC solutions, nl. SITA RFA 2306. This contract supports procurement of turnkey solutions built by approved suppliers from SITA-certified products and components.

4.1 Define user requirement

The end-user requirement for surveillance solutions must be defined in terms of SANS 10222. Annex A has **Camera** and **Solution Requirements Checklists** to help define the requirements per site.

These Checklists must be published along with the RFQ/RFP to enable suppliers to propose complete and suitable solutions.

If a suitable surveillance expert is available (either from SITA or the Department) a preliminary solution design and bill of quantities (BoQ) can be drawn up to be published in the RFP.

- 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).
  - Physical parameters such as the position of gates, fences and walls must be taken into account, as well as distances between points: for example, a camera mounted at the gate must be within the POE distance limitations specified by the OEM or determined by the equipment and cabling.
- Verify **appropriate sizing** of the requirement before publication. Elements that must be sized include network equipment (number and type of ports on LAN switches), storage for footage and network bandwidth.
  - Network equipment must be included in the SAC solution unless existing switches have sufficient POE and port capacity.
  - Network bandwidth is determined firstly by whether recording and triggering are done centrally or at the edge. For centralised recording, insufficient bandwidth can cause delays, packet loss, poor video quality and data corruption. Ultimately this impacts the final success of the system: if the video quality is poor, the system will not achieve its goals. Bandwidth is impacted by the number of cameras, video resolution and video compression codecs.
  - Storage of captured video is one of the final steps in ensuring a successful surveillance system. If the storage is too slow or has insufficient capacity, capturing or retrieval of footage could be compromised. Firstly a decision must be made on the length of time that footage will be retained. Secondly the amount of storage required for each camera must be determined, and multiplied together with the total number of cameras will result in the total amount of storage. Future expansion must also be catered for to ensure that the system can grow as needs change.
- Approach SITA for **advice** (if required).

4.2 Publish RFP

An RFP containing the business requirement and evaluation criteria is published and responses gathered via the appropriate SCM process.

The RFP must include the following information in order to ensure a complete description of the business requirement:

- Overview of site surveillance/access control requirement
- Camera Checklists
- Overall business requirement Checklist
- Site floor plans (if not classified, as in the case of National Key Points, for example)
- Any existing infrastructure or systems that must be integrated into the solution
- Special or unique requirements that must be catered for
- Preliminary BoQ (if available)
- Data retention policy: time period that video footage must be retained
- A list of **evaluatable**, mandatory and quantifiable business criteria. This includes for example requirements for additional components, services such as regional delivery, installation and maintenance, or upgrades from the base specification to meet additional performance requirements.

4.3 Site inspection

The RFP specification must include a date for the formal site inspection. All suppliers have the opportunity to attend the site visit (which may include a briefing session); failure to attend means that no response will be acceptable from that supplier.

4.4 Evaluate proposals

Supplier proposals are evaluated according to the relevant Departmental processes. The following mandatory criteria must form part of the evaluation.

4.4.1 Mandatory criteria

- Supplier accredited on RFA 2306 (SITA confirmation)
- Supplier accredited for the province (SITA confirmation via RFA 2306)
- Supplier PSIRA-accredited (current, valid PSIRA certificate)
- Supplier accredited for the relevant SAC category: CCTV integrators may not excel at supplying access control solutions (OEM confirmation)
- Supplier OEM-accredited per brand (OEM certificate)
- Supplier must be capable of supplying, commissioning and maintaining a solution of the required scale
- Supplier must have available on staff (or sub-contracted) all the necessary skills and resources (e.g. electrical engineer)
- Security clearance: supplier personnel must have the appropriate level of security clearance as required by the project and/or client department
- Surveillance and access control devices SITA-certified – e.g. cameras, readers, NVRs, etc. (SITA product certificates)

- All solution elements in the URS must be addressed: proposed solution must meet all stated requirements (check proposals)
- All required infrastructure for solution such as networking, backup power (e.g. solar, UPS or generator), equipment racks, trenching, etc.
- All infrastructure (electrical, civil, etc.) must be done in accordance with SANS standards
- All solution elements costed (check proposals)
- Services that must be bundled:
  - Installation, commissioning, training, support and maintenance.

4.4.2 Disqualify non-compliant bids

Disqualify bids that do not meet mandatories, arriving at a shortlist of solutions that can be evaluated further.

4.4.3 Proposal evaluation

Evaluation of the proposals must take into account the following elements:

- Skills and experience (including PSIRA- and OEM-accredited resources)
  - CVs of skilled and certified resources on staff: minimum 2 years of related experience
- Reference sites: at least 1 site of similar complexity
- Cost comparison: Solution price and cost-effectiveness
  - The RFP specification must enable an “apples-to-apples” cost comparison
- PPPFA or BBBEE

The scoring process must yield a final points total for every bid.

4.5 Award bid

Once the evaluation process is concluded the bid is awarded to the solution that scores the highest total points according to standard procurement processes, taking into account mandatory criteria, empowerment goals and cost-effectiveness/TCO.

4.6 Installation

Complete system with all components must be delivered, installed and implemented according to OEM and industry best practices.

The final responsibility for a fully working solution rests with the supplier/integrator. Any issues with completeness, adherence to requirements, functionality or performance must be resolved by the supplier before the project can be signed off.

All OHS requirements must be met as per SA regulatory framework.

4.7 Commissioning

A formal sign-off process must be done for the solution once it is determined that all business and functional requirements have been met as defined in the RFP. For evidentiary purposes, where required, a complete system image quality test must be performed for surveillance solutions, including an objective, standardised

test for cameras with high-level evidentiary/image quality requirements, with a spot check by an independent auditor.

Other deliverables that must be handed over at commissioning include:

- System design, plans and drawings
- Security setup and system passwords
- Warranty documents for all components
- SLA for entire specified period
- Rotakin/Digikin (ISO 50132) or IEC 62676-based test results (applicable to surveillance systems) as required by the surveillance needs per camera: objective criteria and standardised process for measuring actual recorded image quality, including spatial resolution, image sharpness, focus, light levels and colour accuracy. These evaluations should preferably be done by an independent, qualified auditor.

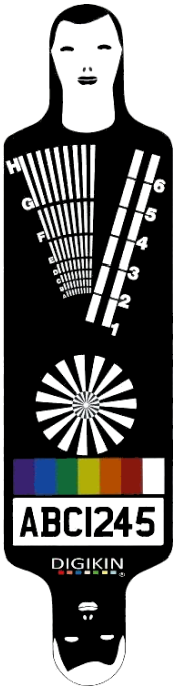


Figure 9: Digikin test target

4.8 Training and consultation

Training of operator and administrator resources of any SAC solution is vital. The following types of training are required:

- Generic SAC training: principles, basic motivations, etc.
- Product- and solution-specific training pertaining to the actual operation of the on-site SAC solution
- PSIRA training also available for integrators: third-party service
- Detail training on entire system for facility and security personnel.

An *ad hoc* consultation service may be required by Government for specific issues, to improve performance or to address new or additional requirements.

4.9 Maintenance and support

The minimum specified service lifecycle for any surveillance or access control system and all its components is 5 years, with a mandatory next business day (NBD) repair SLA bundled.

The maintenance and support agreement must include a regular system performance and video quality verification audit done by the supplier: at least every 6 months for critical sites, and every 12 months for standard (non-critical) sites.

Site audits must generate a report capturing the following elements per surveillance point (camera):

- Pass/Fail w.r.t. stated purpose of camera (e.g. Motion/observation/facial identification)
- Corrective action (supplier or end-user)

All negative audit findings must be addressed to ensure that surveillance footage will provide the required level of quality for evidentiary or other process needs. For example, if recorded video footage does not provide the required legal standard to achieve a conviction in court, the surveillance solution could result in fruitless and wasteful expenditure.

In addition to quality audits, the following maintenance actions must be done on a scheduled basis as agreed with the client:

- Surveillance systems:
  - Test connectivity to all cameras
  - Test remote access to and from VMS
  - Test video playback to ensure the functionality of the recording system
  - Verify recordings
  - Identify and report all faulty lights that can affect surveillance quality
  - Clean lenses on all cameras
  - Correct focus on all cameras as required
  - Reposition all cameras as required
- Access control systems:
  - Integrity test all access readers (biometric, token, PIN)
  - Inspect magnetic door locks for functionality and security
  - Clean all biometric readers
- Query all system logs to determine issues

Findings and actions taken during the maintenance process must be added to the site audit report.

5. Conclusion

The SAC 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 SAC requirements. Following the guidelines in this document should enable Government to deploy SAC solutions to their maximum potential in supporting Departmental physical security 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).

Standards, technical documents and contact details

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

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

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

Annex A: 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: Video Surveillance Solution

This checklist is to be used by Departments to document business requirements when publishing a request to industry for a surveillance solution. The checklist helps to define the parameters and goals for the solution, enabling integrators to provide informed designs and suitable proposals.

Summary of video surveillance business requirement
High-level business need, including what must be protected/surveilled

Site/Project details	
Site / project name	
Location of site: physical address (province, town, street, building, floor, room)	
Site coordinates (latitude,longitude)	
Primary contact person for project	
Contact details (cellphone, e-mail)	
Describe access to site for service provider (business hours / after hours)	
Estimated date for site inspection	
Existing CCTV equipment installed on site, if any	

Number of Camera Checklists completed for site					
Site size classification	Small ☐	Medium ☐	Large ☐		
Floor plans available? (must be included in RFP)	Yes ☐	No ☐			

Functionality required	Tick with ☑		
Indoor / outdoor	☐	Control centre / viewing system	☐
Perimeter security	☐	Video transmission to to central site (archive/backup)	☐
24-hour surveillance	☐	Remote viewing/central control room	☐
Low-light/night surveillance	☐		

Technical requirements							
Backup power requirement – how long must cameras run during power outages							
Envisioned future upgradeability of solution							
Video analytics requirements:	Motion ☐	Intrusion ☐	Heat map ☐				
People counting ☐	Line crossing ☐	Object left/removed ☐	Other:				
Describe security considerations w.r.t. confidentiality of footage							
Describe unique technical requirements, or other points not covered above (if any)							

Requirements Checklist: Video Surveillance Camera

This checklist must be used in conjunction with the **Surveillance Solution Requirements Checklist**, which provides an overall definition of the requirement. A checklist must be completed for every camera required on the site.

Site details	Camera checklist number	001
Site physical address		
Building / floor / room		

Location of camera	Tick with ☑									
Type of location	Indoors	☐	Outdoors	☐	Office	☐	Passageway	☐	Public access	☐
	Secure area	☐	Other:							
Position of camera	Doorway	☐	Corridor	☐	Room	☐	Other:			
Distance from control room / network room (metres)										

Surveillance requirements	Tick with ☑					
What/who is to be observed?						
What is the reason for the observation?						
When is the observation required?						
What activities are to be observed?						
Likelihood of activity occurring	Low	☐	Medium	☐	High	☐
Frequency of occurrence	Occasionally	☐	Regularly	☐	Often	☐

Camera primary purpose (determines image quality)	Tick with ☑							
Observation type required (SANS 10222):								
Monitoring and control	☐	Detection	☐	Recognition	☐	Identification	☐	

Lighting conditions	Tick with ☑									
Camera must function effectively in the following lighting:										
Day	☐	Night	☐	Natural	☐	Artificial	☐	All conditions	☐	

Technical requirements (camera capabilities)	Tick with ☑									
Pan Tilt Zoom (PTZ)	☐	Pano 180°	☐	Pano 360°	☐	Thermal	☐	Other:		
Special features:										
Tamper-proof	☐	Vandal-proof	☐	On-board audio (mic + spk)	☐	On-board LED light	☐			
Licence plate recognition	☐	Face recognition	☐	Temperature screening	☐	IR sensor	☐			
On-board alarm	☐	I/O connectivity	☐	Other:						

Camera infrastructure	Tick with ☑							
Camera mounting options:	Ceiling	☐	Wall	☐	Pole	☐	Other:	
Network point at location?								
Power over Ethernet available?								

Requirements Checklist: Access Control Solution

This checklist is to be used by Departments to document business requirements when publishing a request to industry for an access control solution. The checklist helps to define the parameters and goals for the solution, enabling integrators to provide informed designs and suitable proposals.

Summary of access control business requirement
High-level business need, including what must be protected

Site/Project details							
Site / project name							
Location of site: physical address (province, town, street, building, floor, room)							
Site coordinates (latitude,longitude)							
Primary contact person for project							
Contact details (cellphone, e-mail)							
Describe access to site for service provider (business hours / after hours)							
Estimated date for site inspection							
Upgrade of existing system or new installation?							
Integration required with existing system or devices?							
Existing access control equipment installed on site, if any							
Site size classification	Small ☐	Medium ☐	Large ☐				
Floor plans available? (must be included in RFP)	Yes ☐	No ☐					

Functionality required	Tick with ☑		
Indoor / outdoor readers	☐	Integration with control centre / surveillance system	☐
Perimeter security	☐	Central control room	☐
24-hour access?	☐		

System capacity and capability	
Number of users (current + projected growth over 5-10 years)	
Estimated total number of transactions per day	
Traffic level per door (e.g. front door vs. basement storeroom)	
Peak traffic estimate: highest-volume entrance	
Reliability requirements: Uptime,	

Annex B: Project/Site Sign-off Checklist

This sign-off Checklist provides a procedure for suppliers/integrators and clients/end-users to ensure that all relevant procedures and standards were followed during the project. Every sign-off item on this checklist must be supported with documentary evidence (certificate/photographs).

SITA

Sign-Off Checklist: Surveillance and Access Control Implementation

This checklist is to be used by Departments at the final inspection of a CCTV implementation project to ensure that all appropriate actions have been taken, all mandatory services and components have been delivered and installed, and all required standards have been met.

Each sign-off item on this checklist must be supported with **documentary evidence** (e.g. report, certificate, photographs).

Site and Project Details	
Site / project name	
Implementation address (town, street, building, floor)	
Date of commissioning	
Department representative performing sign-off inspection (name and contact details)	

Camera and Video System (CCTV solutions)	Tick with ☑
SANS 10222 (Rotakin) test performed per camera to confirm operational surveilllance requirements are met	☐
Recording system demonstrated to be functioning as specified	☐
Recording system storage capacity delivered as specified	☐
Video management system (NVR or stand-alone) demonstrated to be functioning as specified	☐
Monitoring and alerting/alarming system (e.g. control centre) demonstrated to be functioning as specified	☐
Physical Access (Access control solutions)	Tick with ☑
Access readers tested and verified individually	☐
Access gates tested and verified individually	☐
Enrollment/registration of all users/tokens/biometrics completed	☐
Access control system demonstrated and fully operational	☐
Network Cabling (if applicable)	Tick with ☑
Full performance test done per network point, using calibrated cable tester	☐
Cable OEM site certificate completed and attached	☐
Ducting, power and communication outlets according to Department, OEM and SANS standards	☐
Patch panels, cable looms and bend radii according to Department, OEM and SANS standards	☐
Infrastructure (if applicable)	Tick with ☑
UPS and equipment Racks installed according to OEM standards	☐

The Checklist can be downloaded from www.sita.co.za/prodcert.htm.

Annex C: 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 procurement process.

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

These questions/criteria can be adjusted to suit specific individual requirements; they do not have to be used as-is, but serve as a guideline and starting point.

MANDATORY	Comply	Do not comply
Bidder must be accredited by SITA as a supplier approved on the relevant transversal contract (e.g. RFA 2306).		
Substantiate: Proof in the form of SITA accreditation letter.		

MANDATORY	Comply	Do not comply
Regional footprint: Bidder must be accredited on the relevant contract for product supply and service delivery (as applicable) in the province where the solution must be delivered/installed.		
Substantiate: Proof in the form of SITA accreditation letter.		

MANDATORY	Comply	Do not comply
Bidders must be PSIRA-accredited to the required level.		
Substantiate: Proof in the form of current, **up-to-date** PSIRA certificate – note that business certificates are only valid for 12 months.		

MANDATORY	Comply	Do not comply
Bidder must be certified by all relevant OEMs to design, supply, support and maintain the specific products offered in the proposed solution.		
Substantiate: Proof in the form of OEM accreditation/partner letter.		

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

MANDATORY	Comply	Do not comply
Supplier skills and experience: at least 2 years of relevant experience		
Substantiate: Attach documents proving required criteria (CVs).		

MANDATORY	Comply	Do not comply
Supplier personnel must be security-vetted as per requirements of client Department and site.		
Substantiate: Attach documents proving required vetting.		

MANDATORY	Comply	Do not comply
Supplier track record: at least 1 reference site of similar complexity		
Substantiate: Attach documents proving required criteria (references).		

MANDATORY	Comply	Do not comply
Solution design, project plan and BOQ must be delivered as part of RFP response. The solution design must document the entire technical architecture of the proposed solution		
Substantiate: Deliver 3 separate documents as stipulated		

MANDATORY	Comply	Do not comply
All services, accessories, upgrades and options required by the solution or 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:		

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
All relevant surveillance and/or access control solution elements must be addressed in the proposal. If the bidder realises that some elements were not addressed in the client’s request, these must be highlighted in the proposal.		

MANDATORY	Comply	Do not comply
The service provider must have a call centre service available to ensure required service levels are met.		
Substantiate: Provide call centre contact details		

MANDATORY	Comply	Do not comply
If a Rotakin/Digikin audit is required as part of the SLA, these audits must be performed by properly certified evaluators.		
Substantiate: Provide appropriate certificates		

MANDATORY	Comply	Do not comply
All relevant Occupational Health and Safety (OHS) requirements must be included in the Site Safety File. This includes, but is not limited to the following: ❖ SHE Policy ❖ Letter of good standing ❖ OHS plan ❖ Fall protection plan (for working at height) ❖ Emergency response plan ❖ Risk management procedure ❖ Safe work procedures ❖ Incident investigation procedure		
Substantiate: Supplier must be registered and certified to be in good standing with OHS, and must produce all deliverables listed above as part of the project.		

Annex D: 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	Model	Qty	Unit Price (X VAT)	Nett Price (X VAT)
SAC solution, including:				
Cameras				
Video recorders with integrated storage				
Video management system (VMS)				
IT: compute elements as required				
IT: storage elements as required				
Network component (wired and wireless equipment)				
Power component (UPS/generator)				
Housing component (equipment racks)				
Connectivity component (cabling infrastructure)				
Monitoring component (control room and sensors)				
Surveillance and access control solution, including:				
Access control readers				
Access control system				
Physical access control devices (gates/booms/turnstiles)				
General components:				
Software component (deployment, configuration and management tools)				
Delivery and Installation				
Implementation (e.g. biometric enrolment)				
Commissioning (functional verification)				
Standard SLA:				
Support and maintenance (SLA as specified)				
General bundled services:				
Installation				
Support (incl. service desk/call centre)				
Scheduled maintenance				
Training				
Additional services (e.g. optimisation, integration, software installation, data migration)				
Additional logistics (e.g. regional delivery and installation)				
			Subtotal	
			VAT 15%	
			Total VAT Incl.	

To ensure that prospective suppliers have the financial ability to execute on the project, it may be necessary to ask for a 10% bank guarantee as part of the RFP deliverables. Or alternatively, reserve the right to ask for a guarantee as a pre-condition of award.

Annex E: Abbreviations, Terms and Definitions

Abbreviations

AI	Artificial Intelligence
BEE	Black Economic Empowerment as defined by Act 5 of 2000.
BoQ	Bill of Quantities
CCTV	Closed-Circuit Television
CPU	Central Processing Unit
DCDT	Department of Communications and Digital Technologies
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
DR	Disaster recovery
EMC	Electro-magnetic compatibility
ESM	Enterprise System Management
FTP	File Transfer Protocol
GITOC	Government IT Officers Council
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol (Secure)
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPvX	Internet Protocol version (e.g. IPv6)
IPxy	Standard for solid & liquid ingress protection (IEC 60529)
IR	Infra-red
ISO	International Standards Organisation
ISV	Independent Software Vendor
ICT	Information and Communications Technology
IT	Information Technology
IPMI	Intelligent Platform Management Interface
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
NBD	Next business day
NIST	National Institute of Standards and Technology
NT	National Treasury
NTP	Network Time Protocol

NVR	Network Video Recorder
OEM	Original Equipment Manufacturer
OHS	Occupational Health and Safety
ONVIF	Open Network Video Interface Forum
OR	Operational Requirement
OS	Operating system
OSDP	Open Supervised Device Protocol
PACS	Physical Access Control System
PC	Personal Computer
PDU	Power Distribution Unit
PFMA	Public Finance Management Act
PPPFA	Preferential Procurement Policy Framework Act
PSIRA	Private Security Industry Regulatory Authority
PTZ	Pan-Tilt-Zoom
RAS	Reliability, Availability and Serviceability
RFC	Request for Comment
RFA/Q/P/B	Request for Accreditation/Quotation/Proposal/Bid in terms of a transversal/period contract
ROE	Rate of Exchange
RPV	Remote Piloted Vehicle (drone)
RSA	Republic of South Africa
SABS	South African Bureau of Standards
SANS	South African National Standard
SC-ITSM	GITOC Standing Committee on IT Service Management
SCM	Supply Chain Management
SHE	Safety, Health and Environmental
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
SNTP	Secure Network Time Protocol
SSA	State Security Agency
SSH	Secure Shell
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 SC-ITSM.
UAV	Unmanned Aerial Vehicle (drone)
UI	User Interface
UPS	Uninterruptible Power Supply
URS	User Requirement Specification

VAT	Value Added Tax
VMS	Video Management System
VSS	Video Surveillance System
WAN	Wide Area Network
WAP	Wireless Access Point
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).
Category	A collection of technology Items (products) representing a functional area, such as UPS or 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.
Distributor	Official channel warehousing and distribution, logistics partner appointed by the brand owner.
Component manufacturer	A third-party manufacturer of ICT components that form the basis of complete systems or solutions supplied to Government by OEMs. This includes, for example, CPU manufacturers such as AMD and Intel, drive manufacturers such as Seagate and Western Digital, or software vendors such as Microsoft, Red Hat or VMware. In this domain, components from third-party manufacturers cannot be certified directly via the TCP, 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. Cam_IP2, VMS1. A product must be offered at Item level. Multiple products may be offered for each Item. Items are organised into Categories, e.g. UPS, Racks, etc. (See Category).

Term	Definition
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 32GB storage is specified, 64GB would be accepted, but 16GB 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 – **Next business day repair**: The entire Gauteng Province, as well as in or within 50km from major cities or Provincial capitals, i.e. Cape Town, Gqeberha, Buffalo City, Bisho, Bloemfontein, Durban, Mmabatho, Polokwane, Kimberley, Pietermaritzburg, Ulundi, eMalahleni and Mbombela. Zone B – **2 business day repair**: In or within 50km from major towns, i.e. Naledi (Welkom), Umtata, George, Makhanda, Thohoyandou, Madibeng, Klerksdorp, Ermelo, Standerton, Ladysmith, Oudtshoorn, Richards Bay, Saldanha, Upington, Worcester, Potchefstroom and Beaufort West. Zone C – **3 business day repair**: All towns and rural areas not included in Zone A and Zone B where services may be required. Zone C includes the entire country not covered by Zone A or B. Examples of exclusions to the on-site service requirement include equipment deployed or used on ships or other vehicles, and areas outside the immediate borders the RSA.
Supplier	Final value-added step in the channel before the end user. Compare with Solution provider
"Support for"	A capability that a product must enable, but 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 processing storage,, 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	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 must be done by Suppliers as required to ensure that contracted SLAs are maintained.
Warranty and support	As per detail technical specifications, the following SLA conditions apply to the SAC 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 NBD **repair** (subject to Zone definitions) for **5 years** (60 months) from date of delivery.