INTOSAI

CAPACITY BUILDING COMMITTEE

Managing Information Communications Technology

A guide for Supreme Audit Institutions

This guide has been written by members of the Capacity Building Subcommittee 1 chaired by the UK National Audit Office. This guide is part of a series being produced by the INTOSAI Capacity Building Committee. The series comprises:

1 Building capacity in Supreme Audit Institutions: A Guide;

2 Introducing professional qualifications for Audit Staff: A guide for Supreme Audit Institutions;

3 Peer Review Guide with Peer Review Checklist;

4 How to increase the use and impact of audit reports: A guide for Supreme Audit Institutions;

5 Human Resource Management: A Guide for Supreme Audit Institutions; and

6 Implementing the International Standards for Supreme Audit Institutions (ISSAIs): Strategic considerations.

The guides are in the process of being translated and copies of many of the guides are available in Arabic, Chinese, French, German, Portuguese, Russian, and Spanish – available at: www.intosaicbc.org

Design and Production by NAO Communications
DG Ref: 10675-001

Managing Information Communications Technology

A guide for Supreme Audit Institutions

Contents

Foreword

A core part of managing a modern Supreme Audit Institution (SAI) is ensuring that the organisation has appropriate levels of information and communications technology (ICT) to enable the most efficient delivery of the SAI's functions. In this context ICT covers the services, systems, infrastructure and personnel capabilities that the SAI consumes.

This INTOSAI Capacity Building Committee Guide has been written to help senior managers in SAIs understand what constitutes modern ICT and what they might expect from their ICT services provider, be they internal or external. It will be of use to ICT staff in SAIs to help them ensure that their work is consistent with international good practices. It will also be of use to staff at a SAI who consume ICT services to understand how ICT is managed.

This brief guide cannot cover all aspects of ICT service provision nor give practical examples of how to implement each aspect but it is hoped that it will act as a form of checklist and starting point for SAIs wanting to develop or benchmark this area of their operations. Over time it is hoped that other SAIs will share their tools and add those to the website maintained by the INTOSAI Capacity Building Committee.

I encourage all SAIs to consider this guide carefully, to compare your own current practices and resources, and to consider what, if anything, may be needed to ensure your own ICT management systems are fit for purpose.

I would like to thank the NAO team, Steve Williams, Angus Waugh and Demi Aderibigbe, for producing this guide and all those from across the SAI community who provided input and commented on drafts.

Mr Kimi Makwetu

Chair of INTOSAI Capacity Building Committee
Auditor-General of South Africa

Chapter 1
Introduction

The INTOSAI Lima declaration (ISSAI 1) recognises that an effective Supreme Audit Institution (SAI) is dependent on its capacity to utilise technology to enable the efficient delivery of its services and outputs. Information and communications technology (ICT) refers to technology for storing, retrieving, manipulating, transmitting or receiving information electronically or digitally. Computer hardware and software and other communication infrastructure such as video and telephones, including mobile technology and other emerging communication technologies are part of ICT.

This guide helps identify the key aspects that comprise a modern ICT capability, recognising that it may take some SAIs many years to achieve an optimal level of ICT maturity. It is important to strive for a maturity that is appropriate for that SAI. This desired maturity will be influenced by various factors, including local investment levels, national infrastructure and resourcing constraints. Similarly, ICT is a dynamic and constantly evolving discipline. Regular review of whether the services and systems offered by an SAI's ICT department are the right ones is essential to prevent the ICT services losing alignment with the internal and external landscapes.

IT (Information Technology) and ICT will be used interchangeably in this guide. It is therefore necessary to clarify these terminologies. IT refers to the use of computers, networking, software and other equipment to manage information while ICT integrates IT with communications technology (audio/video processing and transmission and telephony). ICT therefore extends the use of IT to manage information and can be seen as an extended acronym for IT.

The guide covers the following key aspects of modern ICT capability:

- Chapter 2 – Setting up an ICT function.
- Chapter 3 – Developing an ICT strategy and ICT Strategic framework.
- Chapter 4 – Developing an ICT competency framework, and establishing and sustaining ICT personnel skills and capabilities.
- Chapter 5 – Establishing IT architecture as part of SAI's Enterprise Architecture.
- Chapter 6 – Designing and implementing ICT infrastructure and Application Portfolio (and Management).
- Chapter 7 – Ensuring ICT security.
- Chapter 8 – ICT Service Management, measuring the performance of ICT, maintaining and sustaining an effective operating model.

At the end of some of the chapters there are pointers to other relevant resources, which SAIs may wish to access and adapt.

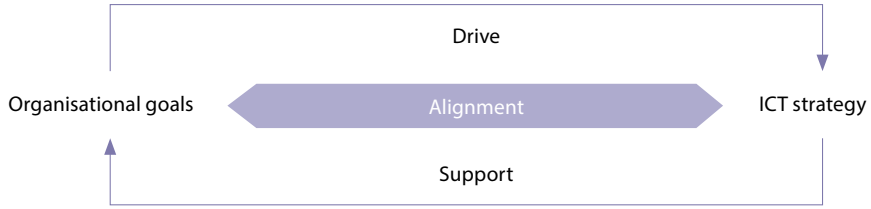
Chapter 2
Setting up an ICT function

An effective and relevant SAI requires a well managed, functioning ICT to deliver organisational objectives. ICT is no longer an option as organisations all over the world are becoming more dependent on computing technologies and even greater dependencies are expected in the future. The ICT department of an organisation exists for three reasons:

- to provide ICT-enabled capabilities to the SAI;
- to steward those capabilities; and
- to help shape and guide business demand for ICT-enabled innovation, enabling the delivery of the SAI's functions.

How does an SAI create, develop and maintain an ICT function that is fit for purpose?

ICT must be viewed as a means to an end – a tool for fulfilling or enabling organisational purpose, therefore the goals of the organisation should drive how ICT is deployed and harnessed by the organisation. While organisational goals come first, ICT strategy developed to align with the goals helps to ensure a focused and effective employment of ICT in the achievement of the goals.



To effectively align ICT strategy to organisational goals, SAIs should break their general goals into a number of more detailed objectives, which gives the respective SAI its own distinctive culture and character. The clearer the SAI can be about what its goals and objectives are, the easier it is to judge how ICT can best fit to achieve those goals and objectives.

Organisational goals and objectives are easily understood when expressed in non-technical terms. SAIs should also ensure that broad organisational goals are broken down into objectives by people who can ensure all relevant areas of the organisation's activities are adequately and effectively addressed and expressed.

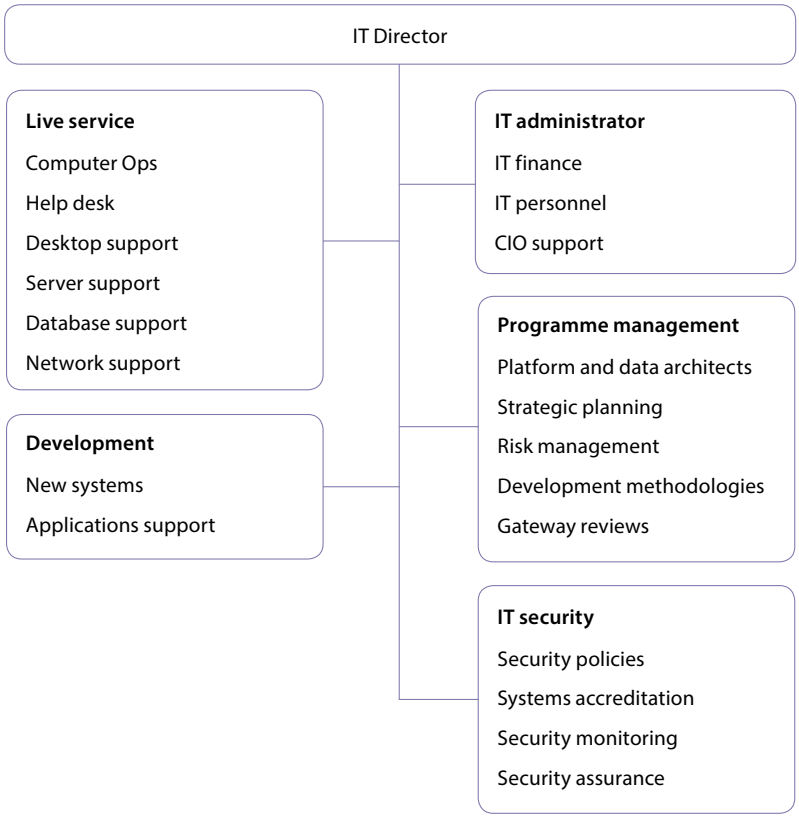
What does an ICT function look like?

A typical ICT Function will have:

- An IT Director, a Chief Information Officer (CIO) or Chief Technical Officer (CTO) reports to senior management and/or the Board.
- The IT Director will typically be supported by: a Live Services manager, Development manager, Programme/Projects manager, IT security manager and IT Administrator: The diagram at **Figure 1** below outlines the responsibilities of each of these managers.

Figure 1
Typical structure of an ICT function

Typical IT organisation



Source: National Audit Office

In reality, ICT structures in organisations come in different shapes and sizes and are very unlikely to be an exact replica of the above 'typical' structure. For instance, in some organisations, the basic/core functions may be collapsed depending on the need and suitability of the organisation. Generally, the large SAIs would have a more structured and defined ICT setting while ICT department of a small or medium sized SAI would be less so with functions collapsed for cost efficiency and to reflect resource availability.

SAIs, especially developing SAIs with less defined ICT functions, should consider putting in place an ICT working group or steering committee. The steering committee provides a rich source of knowledge and strategic support to the IT Director and effectively and robustly bridges the gap between the SAI management and the ICT section to ensure continued alignment of the SAI's business objectives and ICT strategy.

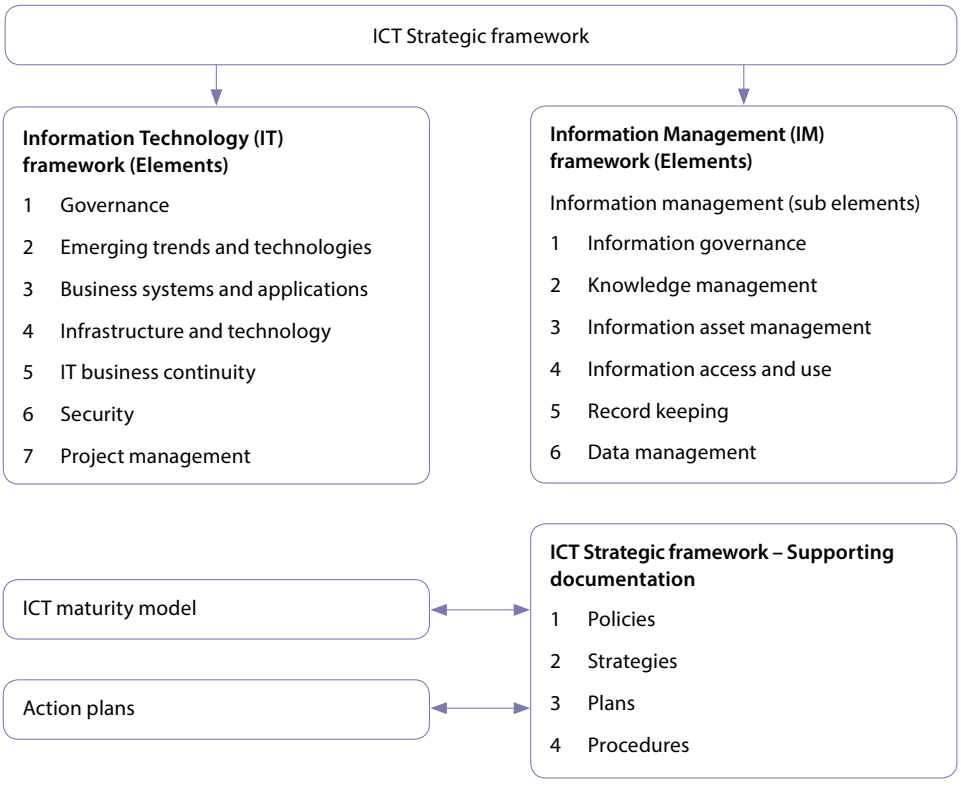
Other considerations by SAIs in setting up ICT functions include:

- Whether the broad goals of the SAI been expressed in clear, specific and detailed objectives and these objectives are at the right level of detail to enable the development of an effective and fit for purpose ICT strategy.
- The level of ICT visibility within the SAI, in particular, whether there is a senior ICT representation.
- Whether there is a structure in place to ensure and continuously monitor the alignment of organisational goals and ICT strategy, and who is responsible for the effective functioning of this structure?
- What level of resources will the IT Director have and to what extent can he/she build teams which can cover the responsibilities and tasks which will need to be performed?

Chapter 3
Developing an ICT strategy and ICT Strategic framework

The SAI should develop an ICT strategy (also known as a Technology Plan) to help ensure that investment in and the use of technology is firmly tied to the organisation's goals and objectives to sustain the present and manage emerging trends. The key to achieving this is through the ICT Strategic framework (ISF). The ISF identifies key elements that are required to be effectively managed to ensure that corporate information and ICT systems are secure, protected, controlled and maintained, see **Figure 2**.

Figure 2
Key elements of an ICT Strategic framework



Source: Government of Western Australia – Department of Local Government – Information Strategic framework

The effective implementation of the framework will result in the development of policies, strategies, plans and procedures to guide the organisation to achieving the desired objectives. In this regard, SAIs are required to give consideration to the **key questions** on the elements of supporting IT and IM frameworks as detailed below.

Element	Details
Information Technology (IT) framework	
Governance	Guiding strategies, principles and practices that underpin all decisions on ICT and guide the correct and effective delivery of ICT. This includes sets of instructions that inform the staff of the SAI about acceptable behaviours expected of those using technology at the workplace (Acceptable use policy). **Has the SAI developed appropriate guiding strategies, principles and practices to support the effective delivery of ICT services?**
Emerging trends and technologies	The emerging trends and technologies such as social media, smart phones and devices, Cloud computing, online services and open data, which provide challenges and opportunities in managing ICT systems and resources, and the delivery of future ICT services. **How is the SAI responding to the challenges of emerging trends and technologies and to what extent will the SAI take advantage of these emerging trends and technologies in the delivery of its services?**
Business systems and applications	The software systems and applications including, software acquisition, software design, software maintenance and management, business process analysis, systems integration, software testing and implementation. **Is the SAI adequately resourced to support, build or buy decisions?**
Infrastructure and technology	The hardware and network infrastructure for delivering ICT services. It covers infrastructure (physical IT hardware such as servers, network equipment), architecture (the design of the infrastructure environment used to interconnect computers and users), virtualisation (the process of creating virtual rather than actual hardware platforms, storages devices or network resources), capacity, communications and network management. **Is the SAI adequately resourced to support, build or buy decisions?**
IT business continuity	Activities undertaken to ensure continuous availability of systems to support the organisation's operations and covers such areas as: disaster recovery, contingency planning, back-ups and data recovery. **Are there adequate arrangements for addressing system and data availability issues?**
Security	Protecting systems and data from unauthorised access, use, modification disclosure or destruction and covers areas including: access management, incident management, change management and physical and environmental security. **Will the planned security arrangements by the SAI be sufficient to protect the systems and data of the SAI and be cost effective?**

Element	Details
Information Technology (IT) framework *continued*	
Project management	Planning, organising, controlling and managing resources to achieve specific goals. Key elements include: project initiation, project planning, project execution, monitoring and controlling and project closing. **Is the SAI building-in appropriate project management methodologies to achieve desired results?**
Information Management (IM) framework	
Information governance	The management and controlling of the current and future use of information. Elements of information governance include: information management strategy and planning; information management policy; principles and architecture; information risk management; and monitoring and compliance. **Has the SAI specifically addressed the need for the management of information to provide assurance that information is available only to the authorised users and only according to the needs of the users?**
Knowledge management	The capturing and the use of knowledge to best effect within the organisation. Elements include: business intelligence; knowledge sharing; knowledge transfer; data mining and analytics; and knowledge retention. **Has the SAI built in adequate capacity and capability to harvest and retain knowledge through organisational learning?**
Information asset management	Identifying and managing information assets of the SAI. Key elements include: registration; information asset classification; and custodianship. **Are there structured procedures in place at the SAI to identify, monitor and maintain custody of strategic assets, including information assets?**
Information access and use	Basis of information access, use, storage and transfer. Key elements include: intellectual property; access and accessibility; privacy and confidentiality; sharing and exchange. **Will there be clear and robust instructions and policies on the basis on which information is accessed, used and shared?**
Record keeping	Keeping and maintaining complete, accurate and reliable records of the entity's activities. Key elements include: record creation and capture; records management; archiving, retrieval and access; and records retention and disposal. **With the increasing use of technology by SAIs, are the existing policies on record management (creation, retention and disposal) adequate or are updates necessary to be fit for purpose?**
Data management	Valuing and managing data as a strategic asset in particular to maintain data integrity. Key elements include: data capture; data integration; data conversion and transformation; and data warehousing. **Is a robust system in place to ensure and maintain the integrity and availability of data?**

The need for strong governance of enterprise IT initiatives, including in particular clear support from the SAI's leadership cannot be overemphasised. It is critical that the SAI's IT functions in alignment with the SAI's strategic objectives and in compliance with its internal policies and relevant external laws and regulations. Essentially, the SAI leadership needs to create an environment that enables compliance and monitors alignment of ICT strategy with business objectives. Part of achieving this include ensuring that the strategy developed states explicitly the SAI's business context and how the IT function will contribute to the achievement of the SAI's success.

Chapter 4
Developing an ICT competency framework, and establishing and sustaining ICT personnel skills and capabilities

Maintaining the right level of ICT human resource is essential to prevent inefficiency and avoid waste. It is a critical success factor to delivering value and leveraging ICT capability efficiently across the organisation. Ensuring that the ICT department of the SAI has the right staff and deploying them effectively is the responsibility of the IT Director.

IT Director

The IT Director is the focal point providing specialist advice, guidance, support, and leadership on all ICT related matters. The person appointed by the SAI as the IT Director should be someone who shares the SAI's vision and can add value to the big picture on how the SAI could function better with the help of technology.

Working with the SAI leadership, the IT Director should align ICT functions with the SAI's business requirements. It is essential that he or she possesses sufficient experience at supporting similar organisations and is attuned to the latest IT developments and so is capable of bringing into the SAI, industry expertise and best practices.

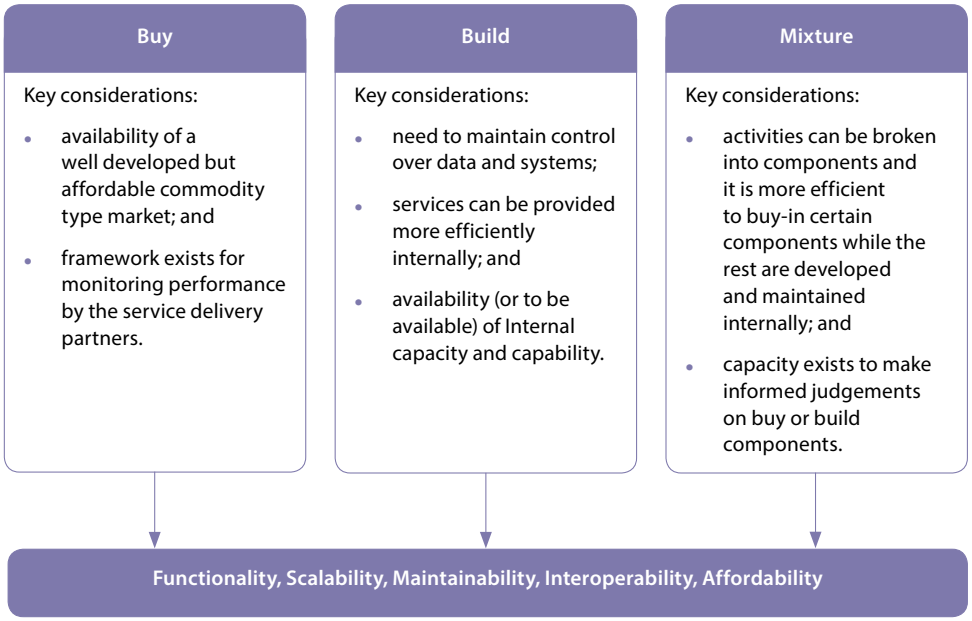
ICT Human Resourcing Capability

The sourcing of provision of service model adopted by the SAI invariably drives human resource capacity requirement and utilisation by the SAI.

Sourcing of provision of service model – Buy, Build or Mixture

The SAI has to make a strategic decision as to the most efficient way of providing ICT services – Buy-in ICT services, use internal resources to build ICT capability or a combination of both, see **Figure 3** overleaf.

Figure 3
Service Provision Model



Source: National Audit Office

Most organisations adopt the 'mixture' model, albeit in varying degrees. Where a high proportion of ICT functions are performed internally, human resource requirements tend to mirror the work demand.

Building an ICT team

As soon as the IT human resource capacity needs of the SAI have been decided (refer to section 2 for what that could consist of), the IT manager should work with the HR department in recruiting staff with the right competences both from within and outside the SAI. Once recruited, especially the external candidates, they now form part of the workforce of the SAI and come under HR management for job appraisal, training, promotion and other HR needs (**See: Human Resource Management – A guide for Supreme Audit Institutions**).

Managing third-party services

SAIs must ensure bought-in services from third parties (suppliers, vendors and partners) are managed to deliver value and meet business requirements. To achieve this requires a clear definition of roles, responsibilities and deliverables in third-party agreements and associated SLAs (service level agreements) which have clearly defined targets for service delivery and the regular review and monitoring of such agreements to ensure effectiveness and compliance.

Maintaining ICT competence – framework

Key to maintaining ICT competence is the availability within the SAI of a robust training, learning and development programme. As laid out in the INTOSAI booklet '**Human Resource Management – A guide for Supreme Audit Institutions**' and with specific application to the ICT staff:

- the **SAI's policy for training and development** should identify relevant individual team and corporate training needs, consistent with organisational goals and be transparent in offering guidance to staff in the development of their careers;
- … during the appraisal interview, the employees and manager should discuss the individual's past performance, future work assignments and career aspirations. After the appraisal the manager will make sure that training needs are met and dealt with;
- developing the training plan for the ICT section would in general be based on the strategy document, individual needs from performance reviews, and training needs, questionnaires and evaluations.

The BCS (British Computer Society), the UK Chartered Institute for IT, has a comprehensive framework for ICT skills (SFIAplus – Skills Framework for the Information Age), covering: strategy and architecture (including information governance, management and security); business change; solution development and implementation; service management; procurement and client interface: http://www.bcs.org/category/17797?src=sfia

Chapter 5
Establishing IT architecture as part of SAI's Enterprise Architecture

Introduction

Technology constitutes one of the elements of any Enterprise Architecture (EA). Other elements include: business strategies; business processes; systems and information flows; and these elements interact in varied degrees to create synergy and maintain competitive advantage and a distinct culture for the respective organisations.

The IT element of the EA also known as the IT architecture (ITA) articulates the policies, principles, services, standards and guidelines, and vendor specific products for the delivery and governance of IT services across an enterprise. ITA is a key element of EA especially in technology driven organisations. Many organisations including SAIs are becoming increasingly dependent on IT to deliver their business objectives.

Many SAIs have transitioned from the traditional ways of working and delivery to an environment that is dynamic and ever changing. To be fit for purpose, the supporting IT has to be flexible, scalable, adaptable and efficient both in cost and quality. An optimum IT architecture should help to deliver these qualities and align the design and implementation of IT/IS capabilities with business processes to achieve the desired organisational objectives.

In establishing a framework, it is essential that ITA, communicates effectively its value propositions, its adaptability to the needs of the business and the changing environment including emerging technologies and as well as the governance arrangements for the delivery of IT capabilities. Some of the key considerations include:

- **An awareness that ITA is not an end in itself**

  It is a mean to an end – to help deliver the business objectives. It is therefore essential to first consider the needs assessment for the business community in order to develop a successful IT solution – the one that aligns to the needs of the business.

- **Need for simplicity of design and adaptability of the system**

  The system should as much as practicable be simple to save cost in the long run and be simple to understand especially by its stakeholders. The simplicity should be complemented by its agility to respond to changing circumstances while remaining cost effective.

- **Whether technology can be standardised**

  Standardised technology among other benefits enables ease of integration and interoperability of systems, allows for economy of scale, which leads to cost savings, reduces complexity and allows for greater support options and improved efficiency. Given these benefits SAIs stand to gain, should they employ standardized technology where practicable, within their IT architecture. SAIs could, for instance, employ standardised technology for software development (both for programming languages and software development practices), database management systems; and desktop hardware and other facilities within the user-workstation environments.

- **Possibility of consolidating and centralising technology resources**

  Consolidation and centralisation of technology resources also leads to improved efficiency and reduced complexity through the elimination of resource silos. Possible areas for consolidating or centralising resources include:

  - **providing a common directory of services for authentication** or implementing a single sign-on service for the users of the systems resources. Obviously, the overriding consideration is suitability for the business; and whether the organisation's information and information assets still remain secure and protected;

  - **the use of a centralised storage solution** (such as storage area network – SAN) instead of multiple file servers. A centralised SAN runs the risk of a single point of failure and SAIs using this system of data storage must ensure appropriate provisions exist to handle equipment failure for continuous and uninterrupted provision of services; and

  - **operating centrally managed IT personnel** to deliver a lean but responsive and consistent IT services across the organisation. In exploring this option, SAIs operating in multilingual and regionally diverse environments would need to consider these constraints in order enable a fit for purpose arrangement.

- **Opportunity for automating system maintenance**

  Automating system maintenance in the IT architecture saves cost through reduced administrative overhead and support. It is therefore in the interest of SAIs when designing their IT systems to consider automating system maintenance especially for operating system patches/updates, application updates; and anti-malware scans to improve and maintain security.

- **Whether formalised strategic partnerships can be established with IT service providers**

  SAIs may find it expedient to enter into formal strategic partnerships with reputable IT service providers to mitigate risk of skills and capacity shortages in certain aspects of their IT arrangements. While the use of specialised IT service providers helps to ensure availability of the best resources to the SAIs, appropriate control measures must be put in place not only to manage and ensure effective delivery of service by these IT service providers but also to ensure that the activities and security arrangements of the SAIs are not compromised as a result of the use of these IT service providers.

Chapter 6
Designing and implementing ICT infrastructure & Application Portfolio (and management)

Introduction

ICT infrastructure refers to all the computer and communications hardware and software used by SAIs to support and deliver their business objectives. In designing an ICT infrastructure it is essential that SAIs ensure right from the inception that the requested IT services are reliable, policy compliant, cost effective and adaptable to changing business needs. To achieve these, SAIs should design the ICT infrastructure to have a good quality of service and be economically efficient and capable of changing in response to the users' requirements. A good quality of service should guarantee services are made available to users when needed and systems failures are promptly and effectively addressed to ensure continuous and uninterrupted provision of services.

Application portfolio refers to a collection of the SAI's software applications and software-based services used by the SAI to attain its goals or objectives. The portfolio will consist of two broad categories of software – systems and application.

Systems software consists of low-level programmes that interact with the computer at a very basic level, this includes operating systems, compilers and utilities for managing computer resources (eg mobile application deployed to employee operated portable devices to enable authenticated access to data and services). Application software sits on top of systems software and includes such things as database programmes, word processors, and web browsers. In addition, depending on the size of the SAI, applications in use may also include ERP (Enterprise Resource Planning), Audit software, Sharepoint, and a host of other applications necessary for the SAI to deliver business value.

These myriads of applications need to be managed for effective delivery and to mitigate against risk of application failure through the implementation of appropriate Application Portfolio Management (APM) solutions.

In designing a fit for purpose ICT infrastructure, SAIs should consider the following issues:

a) Network

Network equipment (eg routers/bridge routers/switches etc.) allows a group of two or more computing devices to interact via a form of communication technology to create a LAN (Local Area Network) and/or a WAN (Wide Area Network) connectivity. Key considerations in the design of a network include:

- **The number and size of fixed sites:** SAIs with multi-site operations would need to give regard to the volume of activities at each location ensuring that more capacity is allocated to locations with high numbers of users. This allows for efficient and effective allocation and utilisation of resources, avoiding overcapacity in low volume centres while at the same time ensuring smooth and continuous provision of services in high volume locations.
- **The nature of the workforce at the SAI – mobile, static or both:** The ways of working of the workforce at the SAIs should play a significant role in the design of the supporting ICT network system. Typically, SAIs would have a core workforce working at clients' premises on a regular basis and the organisation's network capability should be flexible and robust enough to support this group of staff at their various audit locations and at base, when back in the office.
- **The level of resilience required for WAN links:** SAIs operating in multi-site environments (including links to data centres and other remote working capabilities) must ensure that appropriate resilience is built into the system to prevent undue interruption to the organisation's operations in the event of equipment failures while simultaneously balancing the need for resilience with cost effectiveness to prevent waste and ensure efficient resource utilisation.

b) Servers

Servers manage network resources and are usually located in one or more data centres. These can be either on-site (typically in the SAI's head office) or off-site, either in a dedicated data centre operated by a third-party provider or using an internet (or Cloud) based provider. Key considerations regarding servers include:

- **Whether servers will be physical (dedicated computers managing network resources) or virtual (services provided remotely by third parties) or a mix of physical and virtual:** The level of investment in server equipment will depend on whether these services will be performed in-house. Where practicable, these services should either be fully delivered in-house or be fully virtual. This way, a standard can be developed for managing these services in a cost effective and efficient way.
- **Type of hardware to provide server services:** As far as practicable, SAIs should opt for common hardware, especially where these are to be managed in-house as it is much easier to source for and recruit resources to develop and manage these servers.

- **Whether the servers would have dedicated roles or be multi-rolled:** Network functions performed by servers include storing files, managing printers, managing network traffic, processing database queries, managing web and mail activities, managing applications etc. Depending on the size and the volume of activities of the SAI, each of these functions could be performed by different servers, in which case the servers have dedicated roles and only perform their assigned server function. It is also possible, especially in a low volume, small SAI for a single computer to perform all the server functions or be multi-rolled. SAIs have to decide on which option to employ to deliver their ICT capability efficiently and effectively.

c) Data Storage

When designing ICT infrastructure, key considerations regarding data storage include:

- **Volume of client/corporate data to be stored:** SAIs need to make appropriate and adequate provisions where large volumes of data retention are anticipated. By the same token, data storage capacity excess to requirement leads to waste. A more effective use of resources anticipates volume and procures capacity to match volume while ensuring the system remains scalable to accommodate future growth.
- **Existence of data retention policy:** the volume of data to store will also be driven by how long the SAIs wish to retain documents/files as codified in the SAI's data retention policy. Regular review and updating of the policy ensures data is retained only in line with the needs of the business resulting in the efficient and effective utilisation of the SAI's resources.
- **The level of resilience required for data storage:** Data availability is essential for the smooth operation at the SAIs and, in the design of data storage, SAIs need to ensure that appropriate provisions are in place to ensure continuous availability of data while keeping data redundancy to a minimum.

d) Client Devices

Usually consisting of PCs/laptops and printers connected by Local Area Networks (LANs) operating through the premises occupied by the organisation. However, these can be supplemented by Remote Access Service servers to support remote (client-based or home working, via dial-up or preferably broadband internet access), on-premises wireless (Wi-Fi) access to support flexible working/hot-desking arrangements and mobile (for smartphone/tablet based computing for staff who are on the move or at clients. Key considerations regarding client devices include:

- **Extent to accommodate many devices to access services and data:** Resulting from emerging technologies and the need for greater productivity and flexibility, there is a general move by organisations to seamlessly access services and data from multiple devices, while maintaining enterprise security and remaining cost effective. In addition to the traditional client computing model, other alternative technology, including handhelds and tablets, now feature as part of tools used regularly by an SAIs' workforce. Therefore, in developing their ICT Infrastructure, SAIs should consider the extent of the need to incorporate and accommodate multiple devices in delivering their business objectives.

- **Interoperability of connected devices:** SAIs intending to operate multiple devices also need to take into account the ability of these multiple devices to work with, and as part of a system, to guarantee good quality of service ensuring that users have access to services and data when needed.

e) Communications

ICT infrastructure also incorporates a SAI's communication facilities – fixed and mobile lines, fax, instant messaging, video conferencing etc. Key considerations regarding communication facilities include:

- **Extent of use of IT to support internal and external communications:** The SAI's strategy regarding internal and external communications should drive its communication infrastructure – Public Switched Telephone Network (PSTN), IP(Internet Protocol) Telephony or Unified Communications (the integration of real-time communication services such as telephony (including IP telephony), desktop sharing, data sharing, instant messaging, video conferencing, presence awareness etc). To make these decisions, SAIs need to have decided how best to employ communication infrastructure in achieving their objectives.
- **Whether services will be provided in-house or managed by external providers:** Depending on the availability of capacity and capability together with cost effectiveness considerations, SAIs may decide to develop and maintain their communication infrastructure in-house or contract this out to managed service providers (MSPs).

f) Security

- Web-facing servers hosting internet services (published reports etc.) will need to be protected by dedicated firewalls. Firewalls will also be deployed to protect the internal servers, including those hosting any intranet services used within the organisation.
- Remote access to the organisation's internal systems by staff working at clients or from home should be via a VPN (virtual private network) in order to ensure that their access is authenticated and sessions protected from interception.
- Any wireless access provided in the organisation's premises should be configured so that the wireless traffic is encrypted and visitors/by-passers cannot eavesdrop on internal sessions, intercept internal traffic or access internal systems.
- Desktop equipment (PCs/laptops/mobiles) should be encrypted as should any removable media, and all computers should be configured to prevent the use of non-encrypted removable media.
- SAIs using the Cloud hosting options are required to put in place further checks and balances relating to the requirements for data security and privacy, location of data storage and control of access to these data locations.

g) Disaster Recovery and Business Continuity

- **Disaster Recovery (DR)**: The organisation should consider what arrangements will be required to maintain its ITC services in the event of a major systems failure or disaster:

  Cold, Warm or Hot standby at an off-site data centre?

  Cold means that there is equipment at an off-site DR centre, but the systems will need to be built/configured and the data from the most recent backups loaded before failover can commence. Note that any transactions made after the latest backups were taken will most likely be lost and therefore will have to be re-keyed.

  Warm means that the DR systems are maintained to mirror the live ones but the data still needs to be recovered and loaded from the latest backup tapes before failover can commence and services restored and, as above, any transactions made after the latest backups were taken would have to be re-keyed.

  Hot means that both systems and data are mirrored (using replication software to automatically copy system changes and data synchronously) to the standby DR centre's systems so that failover can take place with minimal delay and services can resume with little or no data loss or any need to re-key transactions made since the latest backup was taken.

  The organisation will also have to ensure adequate connectivity to the DR centre so that staff can access the services there if failover is invoked.

  Plans for failover to DR (and for failback when processing at the primary data centre can resume) should be drawn up and tested on a regular basis.

- **Business Continuity Planning:** The organisation should also have arrangements in place in the event that the premises become inaccessible. There should be provision for staff to be able to go to standby premises which have sufficient desktop infrastructures in place and adequate connectivity to the primary data centre or, if that were to simultaneously suffer a major disaster, to the DR centre. Plans should be drawn up (and held off-site) for invoking such arrangements and should be regularly tested.

Key considerations for application portfolio and management include:

- Whether the application portfolio of the SAI sufficiently takes account of the upstream dependencies (ie business process, functions) and downstream dependencies (ie infrastructures) to ensure continuous provision of services and alignment with business objectives.
- Whether SAIs have installed suitable Application Portfolio Management solutions to identify and eliminate redundant applications and provide transparency into the current catalogue of applications and their linkages to the SAI's business capabilities, strategies and goals.

Assessment of cost and benefit from the use of ICT.

It is essential that ICT services provided to SAIs are cost effective and deliver net benefit to their respective organisations. To achieve this, the leadership of SAIs need to provide an appropriate level of challenge to ICT managers regarding investment in ICT. The ICT managers must be able to demonstrate that the delivery options (Infrastructure, Application portfolio and other ICT delivery components) advised by ICT managers take account of the needs of the business and provide the best value to the SAI.

Chapter 7
Ensuring ICT Security

Apart from legal (data protection, anti-money laundering) and government requirements for data security which public organisations must comply with, SAIs face additional factors concerning the trust of clients and stakeholders in their ability to secure the data they need to obtain in order to conduct their statutory duties. A SAI will need to identify the security required to gain accreditation for access to government networks and systems and may wish to consider obtaining accreditation to international security standards such as ISO 27001. There may also be commercial/industry standards which the organisation has to meet.

The following aspects of IT security should be considered:

a **IT Security Policies:** the organisation should have sufficient policies which specify to staff what systems and data should be secured and what is acceptable and unacceptable behaviour when using the organisation's systems and data.

b **IT Asset Management:** the organisation should have the systems in place to track the IT assets it has acquired and in particular to enable it to ensure that disposals are authorised and don't allow data to be lost or stolen.

c **IT Risk Management:** the organisation should have procedures and processes in place to identify and monitor IT risks and manage issues as they arise. These should be included in the organisation's overall risk management process and escalated depending on the nature and scale of the threat which they pose to the organisation.

d **Compliance:** the organisation should ensure that procedures and processes are in place to monitor and ensure compliance with IT security policies and procedures.

e **Physical Security:** this applies to any premises with access to systems and data and includes locks on doors and windows, security guards, visitor/contractor escort and CCTV surveillance, proximity cards/readers on doors, turnstyle doors and combination locks to computer and communication rooms, etc.

f **Environmental Security:** this applies primarily to data centres and computer/communication rooms and includes air conditioning, fire and flood prevention/detection systems, UPS (uninterruptible power supplies), fireproof safes for back-up and archive media, etc.

g **Network Security:** this applies to the LANs and WANs used/operated by the SAI. In addition to the aspects of security discussed in Chapter 6, they include the physical and logical security of network equipment, firewalls and servers, and of network access points.

h **Operating System Security and Database Security:** systems and databases should be configured and administered so that access is restricted to those system administrators whose job it is to support the applications used by the organisation and unauthorised access is prevented. Direct access to databases should be restricted to database administrators; any reporting should ideally be run on a mirrored management information database.

i **Desktop Security:** user account maintenance, password/login security settings, system access rights.

j **Application Security:** user account maintenance, password/login security settings, access rights to system functions and segregation of duties.

k **Data Security:** data security classification, back-ups/restores, encryption, two-factor authentication, user access rights.

l **IT Service Security:** the organisation should determine the data recovery and business continuity arrangements required to ensure continuity of service.

Standards: In order for security standards to be met in each of the above areas the organisation may wish to refer to or adopt one or more of the following frameworks for managing IT risk and security:

- **ISO 27001 (International Standards Organisation's Standard for Information Security):** http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- **COBIT (Control Objectives for Information Technology)** from ISACA (the Information Systems Audit and Control Association): http://www.isaca.org/COBIT/Pages/default.aspx
- **ISF (Information Security Forum):** 2013 Standards of Good Practice for Information Security): https://www.securityforum.org/shop/p-71-167
- **COSO (Committee of Sponsoring Organisations of the Treadway Commission)** Guidance on Internal Control, 2013 Integrated Framework: http://www.coso.org/IC.htm

Chapter 8
ICT Service Management – maintaining and sustaining an effective operating model, and measuring the performance of ICT

To ensure continuous provision of IT services and maintain the quality of services provided; protect information assets and prevent reputational damage resulting from IT security breaches as well as meet internal and external stakeholders' expectations, providers of IT services must establish, implement and operate effective IT service management processes and controls to manage IT resources and provide assurance for value delivery.

In developing an effective system of managing ICT by SAIs, consideration should be given to issues raised in the following key areas:

Service support

An effective service support arrangement ensures that the users of IT services have access to the services to support the business functions. In addition, the system in place should also ensure that issues raised through the system users' experience are captured, followed up and resolved, to improve the system and enhance subsequent users' experience.

In this regard, SAIs in the design and implementation of their service support arrangement should address the following key questions:

- Is there a single contact point for end users having problems operating the system and is this contact point widely disseminated within the organisation?
- How are the issues raised through the Service Desk Function picked up by the back-office and worked on?
- Is there a robust system in place to prevent leakages through the system and provide assurance that all incidents are captured, reported and followed through?
- Is there a policy regarding the turnaround of incidents raised and is a robust line of communication maintained with the end user while the incident is still live?
- Are there established procedures and arrangements regarding the identification and the handling of system improvement (problem and change management) and system configuration changes (configuration management)? Are these arrangements robust enough to ensure continuous provision of services and prevent risk to the system as a result of unauthorised or badly implemented changes?

Service delivery

Service delivery arrangements ensure the SAI's ICT adequately provides support to the SAI's ICT users. Components of ICT service delivery include: service level management; capacity management; availability management; financial management; and IT service continuity management.

In the design and implementation of an effective service delivery arrangement, SAIs should give regard to the following key questions:

- Whether IT services are provided in-house or by third parties, are there robust service level agreements (SLAs) and operational level agreements (OLAs) that define the levels of services required to support the business and are there clear targets and deliverables which can be measured and reported?
- Is there in place an annual infrastructure growth plan? And is this robust enough to anticipate and incorporate business IT needs and ensure appropriate capacity exists to accommodate the IT resource needs of the organisation?
- What arrangements are in place to monitor and provide assurance of systems' availability in accordance with the conditions of the respective SLAs? Specifically will the monitoring be done through a centralised solution/dashboard or through the use of in-built proprietary systems or both?
- Are the costs of IT services reviewed for cost effectiveness and evidence of value for money?
- How robust is the level of the equipment maintenance contract supporting key IT equipment – Servers, Data Storage etc. to ensure prompt and effective response to equipment failure so that equipment can be brought back to life quickly and with minimal interruption to service delivery?
- What are the arrangements in place to ensure continuity of IT service in the event of serious equipment failure or disaster? And are these cost effective?

Depending on size and capability, SAI's have to decide which part of IT service management to perform in-house and which to outsource (**Refer to Chapter 4 for Buy or Build considerations**). Where services are outsourced, SAIs need to address the above issues with the respective outsourced partners to avoid gaps in the management of IT services.

Standards: The organisation may wish to refer to the following standards for IT service delivery:

- **ITIL (IT Infrastructure Library):** http://www.itil-officialsite.com/
- **ITSMF (IT Service management Forum):** http://www.itsmf.co.uk/
- **COBIT (Control Objectives for Information Technology)** from ISACA (the Information Systems Audit and Control Association): http://www.isaca.org/COBIT/Pages/default.aspx

Acronyms and abbreviations

CIO	Chief Information Officer
CTO	Chief Technology Officer
DR	Disaster Recovery
EA	Enterprise Architecture
ERP	Enterprise Resource Planning
ICT	Information and Communications Technology
INTOSAI	The International Organisation of Supreme Audit Institutions
IP	Internet protocol
ISF	ICT Strategic Framework
ISSAI	International Standards of Supreme Audit Institutions
IT	Information Technology
IT/IS	Information Technology /Information System
ITA	Information Technology Architecture
LAN	Local Area Network
MSP	Managed Service Provider
OLA	Operational Level Agreement
PSTN	Public Switched Telephone Network
SAI	Supreme Audit Institution
SAN	Storage Area Network
SLA	Service Level Agreement

Further copies of this guide are available on the
INTOSAI Capacity Building Committee website:
http://cbc.courdescomptes.ma/