GTAC Analyse Assess Activate
Strategic & Technical Advisory
National Treasury
REPUBLIC OF SOUTH AFRICA

# 2020

# Provision, Utilisation and Management of Information and Communication Technology

# A Spending Review of the South African Police Service


## STUDENT NAME: BUTI VELISUBUHLE

## CLUSTER: JUSTICE AND PROTECTION SERVICES

## NATIONAL TREASURY


SAVINGS@WORK
GOVERNMENT SPENDING REVIEWS

# Table of Contents

## Abbreviations and Definitions

**CIMS:** Case Information Management System

**CJS:** Criminal Justice System

**CRM:** Criminal Record Management

**FMLOB:** Financial Management Line of Business

**IJS:** Integrated Justice System

**ICT:** Information and Communication Technology

**JCPS:** Justice, Crime Prevention and Security

**OCJ:** Office of the Chief Justice

**OECD:** Organisation for Economic Co-operation and Development

**SAPS:** South African Police Service

**SITA:** State Information Technology Agency

**TMS:** Technology Management Services

### Definitions

**ICT:** The United Nations Educational, Scientific and Cultural Organization (UNESCO) defines ICT as a diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.) (UNESCO 2006, p.3).

**Spending Review:** has two main purposes: to give the government improved control over the level of aggregate expenditure, and to improve expenditure prioritisation (OECD 2017, p.34).

# 1. Executive Summary

The following report provides a spending review of ICT in SAPS. Given the strategic role of ICT for the department, there was a need to conduct a review which will assess whether ICT is provided and managed in a cost effective and efficient manner. The provision and utilisation of ICT is an interesting area of investigation given the rapid changes in technology, its impact on financial resources and government being a significant consumer of ICT. After detailed analysis of the evidence obtained from various sources, the spending review has identified the following key findings.

**Provision and utilisation**

1. The review has found that SAPS is heavily reliant on SITA even though there are certain legislative provisions which allow the department to procure ICT systems from external parties other than SITA. There is a need for the department to conduct a detailed assessment on whether it is cheaper and effective to utilise SITA relative to private ICT firms.

2. There is a significant mismatch between the total costs of providing, developing and maintaining ICT systems reflected in the department's audited financial statements and those submitted to the National Treasury for the spending review. This is also applicable to software licence fees paid by the department. This indicates that the department has either under reported its spending on ICT systems or is overpaying SITA and external ICT companies.

3. There is a misalignment between utilisation of ICT systems and performance in some functions of the department. The investment made on ICT is not fully supporting operations and activities in the department.

4. The department is under-investing in ICT systems that could improve service delivery and promote smart policing techniques. This is evidenced by high spending on maintenance and software costs for some administrative systems than core service delivery systems.

5. The department needs to improve business operations in certain divisions such as *Detective Services*. Spending on ICT equipment is poor in this environment and this affects effective implementation of the criminal justice system strategy.

**Governance and management**

6. ICT governance arrangements in the department are met with challenges. Among these is lack of internal controls in the procurement of ICT goods and services and non-compliance with legislation related to supply chain management. This affects spending outcomes and results in adverse audit findings.

7. The review has found the need for the implementation of an Enterprise Efficiency model in the department. This will assist and enable digital transformation.

8. The department needs an ICT product and service lifecycle management strategy. The strategy will entail regular monitoring and evaluation of all assets and network sites as

well as ICT services. This will provide an accurate reflection of the value of all the department's assets and network sites.

**Integration**

9. Case Management systems have been found to play an important role of enabling the exchange of data with other institutions in the criminal justice system yet the department only has 880 (out of 1 154) police stations with functional criminal record and case information systems. Only 60 police stations have the Automated Fingerprint (AFIS) system. Therefore, the integration of systems is not yet at an optimal level in the department. This creates delays and inefficiencies in the finalisation of investigations.

10. The Department of Home Affairs has implemented an ICT modernisation programme which can be used as a best practice model in the Justice, Crime Prevention and Security (JCPS) cluster. Home Affairs has managed to implement the programme with less ICT costs compared with departments such as SAPS. SAPS can also improve digitisation of its service by learning from Home Affairs.

## 2. Introduction

This report provides findings from the spending review conducted on the provision, utilisation and management of ICT in SAPS. The purpose of the spending review was to assess the extent to which the department is effectively and efficiently utilising and managing its ICT to achieve improved performance outcomes. Institutions such as SAPS utilise technology and other systems for the enhancement of their operations and achievement of service delivery objectives (Strom 2016, p.1; Chan 2001, p.139; Albrecht and Das 2011).

Effective and efficient utilisation and management ICT becomes difficult to measure if the risks and benefits are not clear. In the criminal justice system environment, technology and information systems allow law enforcement agencies to effectively manage and minimise crime (Dialsingh 2007, p.222). These benefits, however, do not always trickle down to service delivery beneficiaries in communities. This is evidenced by challenges around low detection rate, network operational challenges, poor case flow management, and limited number of police stations with functional ICT systems (SAPS Annual Reports). Among the key findings from the spending review conducted on ICT in SAPS are that there is poor optimisation of ICT in the department, misalignment between ICT with certain operations in the department, lack of internal controls, and over reliance on SITA for the provision and management of ICT services.

The report is structured as follows. Section 3 provides the context for the spending review on ICT in SAPS, specifically outlining why such a review is necessary. Section 4 outlines a methodological framework adopted in the spending review. The selection of the framework was informed by the nature of the study, alignment with set objectives and the relevance of the study within ICT research. Section 5 provides a high-level literature review and selected case studies from countries that have implemented spending reviews on ICT. The author adopted a purposive approach in selecting the literature given limited studies focusing on ICT provision, utilisation, and management in police departments. A purposive approach allows the researcher to use their judgement in selecting a particular method of study. In an effort to provide a better understanding of the ICT program in SAPS, section 6 outlines the program's

chain of delivery. The main focus is on the key elements of ICT, stakeholder analysis, institutional arrangements, key systems utilised in operational activities, inputs, outputs and contribution of ICT to the department's service delivery priorities.

Section 7 provides a detailed expenditure analysis of ICT. The analysis focuses on key spending drivers, lower level spending analysis in SAPS and benchmarking of ICT costs within the Justice, Crime Prevention and Security (JCPS) cluster. The analysis is informed by public expenditure management principles and analytical methods. These are linked to the overall methodology proposed in section 4. Flowing from the expenditure analysis, section 8 provides performance aspects of key ICT systems in SAPS. The section utilises program evaluation techniques and metrics to assess the extent in which SAPS ICT systems are linked to departmental priorities; the manner in which these systems are mapped to specific elements of operations and performance measures used to track results. The last two sections (9 and 10) provide concluding recommendations and options to improve efficiency in SAPS ICT and generate savings.

# 3. Context for a Spending Review on ICT in SAPS

Information and Communication Technology (ICT) is a critical support function in organisations. UNESCO defines ICT as a *diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.)*. ICT capabilities include:

i) **Planning:** the capabilities that set direction and standards for ICT, Enterprise Architecture and to validate/certify conformance and performance thereto

ii) **ICT integration:** the capabilities that provide and develop ICT Systems and Technology Infrastructure into integrated ICT solutions

iii) **ICT operations:** the capabilities to ensure that ICT Systems and Technology Infrastructure are maintained in a reliable, available and secure environment

Police departments internationally enhance their operational capabilities using ICT inventions and systems (Strom 2017). Technology is essentially viewed as a 'force multiplier' given limited resources in government and objectives of enhancing productivity, improving efficiency and achieving service delivery outcomes. As information is central to what police do in their normal day to day activities, there needs to be systems and processes in place to collect, capture, analyse, store and share the information within the police service and other institutions in the criminal justice system (Jackson et al. 2014, p.1).

The provision and utilisation of ICT is an interesting area of investigation given the rapid changes in technology, its impact on financial resources and government being a significant consumer of ICT.

### 3.1 Problem Statement

SAPS is among the biggest spenders in government with respect to ICT i.e. hardware, software and general IT services. Expenditure on ICT constitutes approximately 20 per cent of the department's non-CoE expenditure. Information obtained from the State

Information Technology Agency (SITA) indicates that in 2019/20, the South African government spent an estimated R20 billion on ICT. In the same year, SAPS spent an estimated R3.8 billion (excluding personnel related costs) on ICT which represents 19 per cent of the total spending on ICT in government in 2019/20.

Under goods and services, computer services is the third largest cost driver after fleet services and operating leases. An analysis of spending at the lowest level under this item shows that the main cost driver is SITA related costs for software licence fees, data lines, internet charges, and network related infrastructure for the department. The provision, utilisation and management of ICT in criminal justice institutions is vital for promoting safety and security. Whether this is done in an effective and efficient manner is subject to investigation.

### 3.2 Objective of the study

The objectives of the study are to:

a) Conduct an ICT spending review in SAPS to better understand spending patterns, consider institutional factors that inform/influence spending in this regard, and recommend alternative options that can be considered to effectively and efficiently manage and utilise ICT in the department.

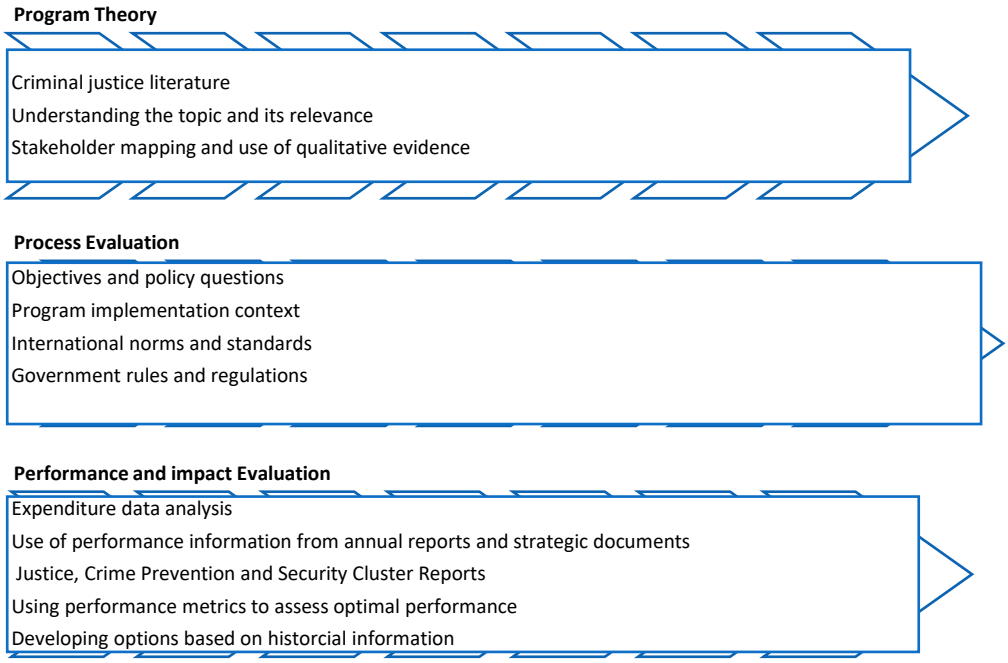
b) Benchmark ICT related costs in the department with those of other departments in the Justice, Crime Prevention and Security (JCPS) Cluster with the aim of identifying possible inefficiencies and best practice that can improve ICT expenditure decisions.

c) Identify possible efficiency savings from various ICT spending areas.

## 4. Methodology

The type of spending review and program evaluation being conducted influences the method of data analysis selected. To unpack the findings, the following flow chart demonstrates the thought process that was followed and elements of data analysis which informed the spending review.

**Figure 1. Data review and analysis flow chart**




### 4.1 Data analysis

The review adopted a quantitative and qualitative approach within the ***Enterprise Efficiency Framework*** of ICT to collect and analyse the data. This framework outlines key components of ICT in an organisation with the goal of mapping adequate provision and utilisation of ICT together with its key elements, and the capacity of ICT to meet the organisation's strategic objectives (Lauras, et al 2015; Government of Western Australia 2016; OECD 2017). These elements have been used to track the acquisition, development, utilisation and maintenance of ICT in SAPS.

### 4.2 Enterprise Efficiency Framework

The Enterprise Efficiency Framework has six elements which are: governance, emerging trends and technologies, business systems and applications, infrastructure and technology, IT business continuity, security and project management (Government of Western Australia, 2016). These elements are briefly described as follows:

**Table 1. Elements of Enterprise Efficiency Framework**

| Elements | Description | How to assess successful application and befits |
|---|---|---|
| **Governance** | This element measures whether ICT provision, utilisation and management in organisations has sound process governance and a customer-centric focus. It promotes efficiencies in ICT governance arrangements. | ▪ Supports digital transformation in organisation and enhances efficiency<br>▪ Seen by the manner in which ICT is well integrated in organisational processes |

| | | |
|---|---|---|
| **Emerging trends and technologies** | Assess emerging ICTs and the manner in which the organisation adopts to technological changes. | Is measured by innovation and adoption of new technologies |
| **Business systems and applications** | This element refers to ICT tools used by the organisation in enhancing productivity and efficient operations. In criminal justice institutions such as the police, crime investigation systems and software fall in this category. | Is measured by performance gaps between ICT systems and outputs delivered by the organisation. Mismatch between the two suggests minimal optimisation of systems and applications |
| **Infrastructure and technology** | Physical hardware such as computers, telecommunications, servers and network points. This element is crucial as it supports data centre optimisation. | Optimisation of infrastructure and technology is measured by the identifying of savings and reducing poorly performing data centres. |
| **IT business continuity** | Relates to effective management and maintenance of IT systems in an organisation. This element promotes the maintaining of plans for the recovery and restoration of the IT systems and to keep them effective through regular testing. | Measured by effective and efficient operations regardless of disruptions. |
| **Security and project management** | Assesses the extent in which data security is maintained in ICT systems. Under this element, availability of critical skills such as project managers, software developers is also assessed. | Is measured by effective cybersecurity, data integrity, and minimal hacking of systems. |

*Source: Government of Western Australia (2016) with author's additions*

Due to the nature of the study, the business systems and applications, governance, infrastructure and technology components of the framework were adopted as they enable an assessment of the efficiencies of ICT resource allocation and also provide methods for assessing guiding strategies, principles and practices that inform the correct and effective delivery of ICT within organisations.

These methods also promote gap analysis on ICT processes, and enable the assessment of structures and processes of the department as they relate to ICT efficiency and effectiveness. Lastly, the framework allows for evaluating how well the outcomes of the department's strategic goals are met and overseen through ICT.

### 4.3 Data sources

Expenditure data for the review was drawn from BAS and the Vulindlela management information system to enable an analysis of ICT spending patterns. The data was also used to benchmark the efficiency of ICT spending across departments in the JCPS Cluster. Performance or non-financial data was sourced from departmental Annual Reports, operational plans and strategic documents, and a literature review on ICT best practices was also conducted.

## 5. ICT spending reviews: case studies and literature review

ICT provision, utilisation and management has several gaps particularly inside and among government departments.

At the outset, the study outlined how SAPS incurs a significant proportion (R3.8 billion) of ICT spending relative to overall government spending (R20 billion). This makes the department a significant consumer of ICT goods and general IT services in government. Yet, as evidenced through annual reports, ICT governance arrangements in the department are met with challenges. Among these is lack of internal controls and non-compliance with legislation related to supply chain management. These also resulted in the department obtaining a qualified audit opinion in the 2018/19 financial year. There are also inefficiencies in areas such as contract management which also led to irregular expenditure incurred in 2018/19 (SAPS 2019, p.300).

As ICT has elements of procurement and supply chain management, the findings outlined in the department's annual report trigger a need to review the manner in which provision, utilisation and management of ICT in the department is implemented. The issues raised in relation to irregular expenditure and inefficient systems in the department call for the necessary steps to be taken in identifying savings.

In the following section, the report outlines two ICT case studies that were conducted to identify savings in different jurisdictions. The selection of these case studies was informed by how they impact criminal justice institutions such as the police and also selected to demonstrate the complexities of identifying savings in an ICT environment.

### 5.1 Case study 1. The United States Financial Management Line of Business (FMLOB) initiative

Citation: ANZSOG 2009; Congressional Research Service 2010

**Project**

Financial Management Line of Business (FMLOB) initiative

**Purpose and time period**

The Financial Management Line of Business (FMLOB) initiative was conceptualised as a ten-year savings project during President George W. Bush's Administration in the early 2000s. Upon being elected, President Bush identified the need to consolidate and modernise ICT systems in government. This was meant to generate savings and improve data quality to support government's decision-making efforts. In 2004, the project was formally launched through the Office of Management and Budget (OMB). The initiative was also meant to streamline and improve efficiencies in common services found across agencies. During President Barack Obama's term (2009-2017), the FMLOB initiative was modified and implemented further.

**Objectives**

To improve the cost, quality, and performance of government financial systems by consolidating agency core systems

Reduce the number of third-party shared service providers (SSPs)

Standardising related business processes across government

**Achievements**

Cost-sharing arrangements across departments on IT were implemented. This involved the transfer of core systems whereby agencies would transfer their core financial system functions such as accounting, payments, and reporting to government-wide shared service providers (SSPs)

The project identified key institutions such as Treasury, Defence, Health and Agriculture to be the central shared service providers (SSPs) of IT systems in government

Systems that are due to end or to be severely modified were identified and addressed

Case Management systems were integrated between the Justice Department enabling exchange of data with other institutions such as the Federal Bureau of Investigation (FBI)

Government wide systems were adopted by consolidating HRM and financial management functions

E-Government Act was implemented in 2014 to enhance reporting and transparency of agencies in data sharing and information disclosure. In the same year, the Federal Information Technology Acquisition Reform Act (2014) was promulgated to improve acquisition and management of Federal IT resources. The Act also provides for acquisition flexibility, process governance and customer-centric initiatives for major IT investments

Closing and optimising data centres is done on an on-going basis. This complies with the Federal Information Technology Acquisition Reform Act (2014)

A dedicated IT Dashboard website was developed to publish cost savings, systems and relevant providers in each government agency. The information on the website (https://itdashboard.gov/) is updated on a daily basis

Performance metrics were developed to track and assess ICT project life cycles in agencies. These metrics are result oriented

The initiative was able to build capacity in agencies to enable them to assess ICT projects, risks and future needs

In 2016, the US Treasury developed a new investment risk rating process and algorithm for reviewing IT investment. This also enables the Treasury to monitor progress on IT performance measures across government.

**Gaps**

Cost-measurement framework was missing. In the early phases of the program, it was not clear how government was going to measure savings on ICT projects

The benefits of ICT and e-government results were not clearly set out. The project was fixated at generating overall financial savings

Following the identification of core institutions and agencies to manage ICT in government, the risks associated with carrying out such functions increased. The cross-sharing of risks was not clearly managed

Internal control weaknesses were not addressed prior to designating some agencies to be the SSPs of ICT

**5.2 Case study 2. Australia's GovNext ICT Program**

Citation: Government of Western Australia 2018

**Project**

GovNext-ICT

**Purpose and time period**

The GovNext-ICT Program is an initiative aimed at reforming Information and Communications Technology (ICT) infrastructure within the Western Australia government by providing the network, cloud and security foundations required. Introduced in 2015, the project is a whole of-government strategy for ICT transformation as it enables government agencies and institutions to consume on-demand and consolidate ICT services. Under the program, government agencies are provided an opportunity to procure ICT services or provide them in-house if there is adequate capacity and resources. The formal launch of GovNext-ICT was done in 2016 with the program being integrated into the Western Australia's ICT Digital Strategy. The strategy has key goals such as: *simplifying technology*; *better connecting agencies and community*; *better informing decision makers, staff and the public* (Government of Western Australia 2018, p.5). GovNext-ICT had a three-year target of generating savings worth AUD65 million across government.

**Program elements:** Telecommunication Services; Data Centres and Associated Management Services; ICT Network Infrastructure Solutions; Servers and Data Storage Devices.

Although the GovNext-ICT program was conducted and implemented at State level, the program was informed by ICT reviews conducted at Federal Level (Government of Australia 2008). These reviews identified the need for a digital transformation, comprehensive ICT strategy, effective and efficient provision of ICT across Australian government agencies and identified ICT skills shortages in the public sector. GovNext-ICT was meant to address some of these challenges in the context of the Western Australian government.

**Objectives**

To modernise ICT functionality and delivery at less cost

To simplify and connect government systems by re-locating physical data centres into pay-as-you-go, secure cloud services

Create a single unified network and modernised telecommunications

To simplify and optimise procurement of ICT infrastructure services

Simplification of the buying mechanism of ICT goods and services to generate savings, increase cyber security and provide agility for government to drive innovation

**Achievements**

The program improved institutional oversight in government. ICT became a strategic government priority. As such, the Office of the Government Chief Information Officer (OGCIO)

charged with overseeing ICT implementation was integrated within the Department of Premier and Cabinet (DPC)

The program promoted upskilling and reskilling capabilities in government and enhanced investment in digital capacity

Government investments on the project yielded results such as enhancing the cyber capabilities framework. This increased Australia's ranking on cyber security

Among its key objectives, the GovNext-ICT program targeted to modernise ICT functionality among agencies. As agencies adopted some of the program elements, trust by citizens in government websites and ICT applications improved (Deloitte 2020, p. 50)

The demand for ICT skilled workers also increased, enabling government to attract skills and compete with the private sector.

**Gaps**

The GovNext-ICT initiative had several weaknesses and barriers

Similar to the US' Financial Management Line of Business (FMLOB) initiative, GovNext-ICT has non-financial risks and benefits that have not been clearly articulated. Agencies are expected to implement the program without a clear outline of the risks and benefits associated with the program

The Office of the Auditor General (OAG) in Western Australia identified issues around assumptions used to develop the program. The OAG argued the program was not realistic as it did not consider Agencies' true ICT needs and costs (OAG 2018, p.6). The program mainly presented 'best savings' scenarios

A significant number of government Agencies in Western Australia were reluctant to implement the GovNext-ICT program. They preferred to continue owning and maintaining their ICT systems.

**Emerging policy issues**

- The two case studies presented above demonstrate the importance of government being clear when setting ICT cost-savings. Participation of all affected agencies is another important factor reflected in both cases. The cases also show the challenges of reducing ICT costs. On the one hand, the US and Australian governments aimed to modernise and consolidate IT arrangements across agencies whilst lowering the spend on the other. The two proved difficult to balance.
- In the case of the US' FMLOB initiative, it is observed that savings on ICT need to be backed by a long-term planning framework. This allows for consultations with stakeholders, institutional planning and for legislative development. The project extended far beyond the ten-year plan set out during the Bush administration. For agencies to start generating and reporting on savings, government promulgated legislation to enforce compliance. There are also strong oversight and monitoring mechanisms from institutions such as the US Treasury. During the development of the program, agencies with less funds were provided with contingency funding to manage and run the systems.
- The FMLOB case presents lessons for South Africa in two dimensions. Firstly, integration and modernisation of ICT systems is crucial for improving data quality and supporting policy decisions. Government decisions need to be backed by sound data

and systems that are well functioning. For savings to be realised, institutions need to identify systems that could be co-shared with other institutions particularly financial and security systems. This promotes collaboration and saves government money. The case also demonstrates the importance of fast-tracking the implementation of criminal justice modernisation efforts.

- However, it is important for government not to be ambitious in setting efficiency savings targets. Savings are not only generated through consolidating systems and functions, but through a careful balance of risks and benefits. As demonstrated in the case, the benefits of consolidating systems were not clearly indicated, making some institutions and agencies reluctant to participate in the process. The risk of managing ICT systems lay with central Shared Service Provider (SSP) departments such as Defence, Treasury, Agriculture, and Health whilst other departments did not share in these risks. Rather, they enjoyed the benefits provided with the new ICT arrangements.
- The Australian GovNext-ICT program also presents some drawbacks on ICT cost-savings initiatives. In the main, governance support structure is crucial for driving cost-saving programs. GovNext-ICT started off as a “bottom-up” program where agencies and institutions were granted an opportunity to focus on consuming ICT services that they need and also consolidate ICT services with other agencies. However, the bottom-up arrangement resulted in a low uptake by agencies. There were no incentives and enforcement mechanisms to encourage participation. As such, the Department of the Premier and Cabinet stepped in and managed the program.
- The case also shows that consultation and ‘buy in’ from all major stakeholders is crucial. This prevents lack of participation by some agencies. Consultation also allows agencies to cooperate and fully declare true costs of their spending programs. As GovNext-ICT was declared as a ‘whole of government’ program, such approach resulted in questionable assumptions applied in the setting of savings targets. The Office of the Auditor General questioned these assumptions and also found over-statement of savings in some instances.

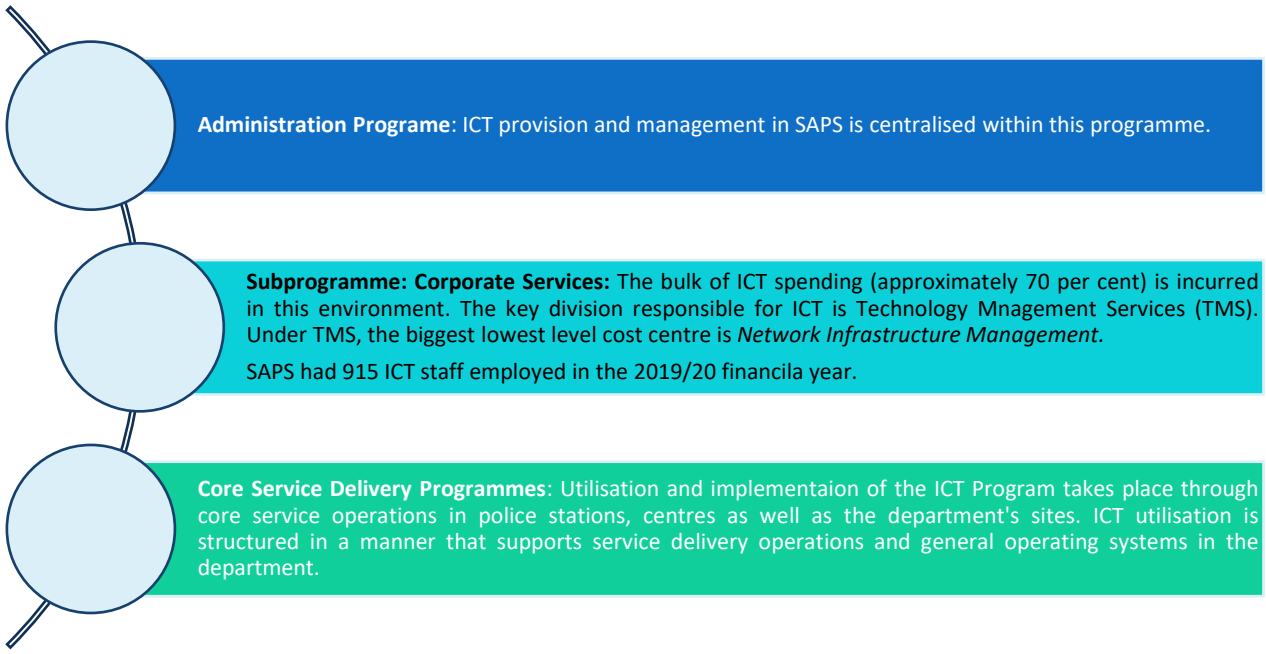
**Implications for SAPS and the JCPS cluster**

- The studies presented reflect the importance of digitising and optimising ICT services. To improve information sharing in the JCPS cluster, SAPS can learn from the Department of Home Affairs and implement some of the initiatives used by Home Affairs in implementing its digital services.
- The case studies have demonstrated that co-sharing of security systems is a crucial aspect of saving costs and creating efficiencies. SAPS submitted data to the National Treasury reflecting 48 different ICT systems. A review of these systems will assist in the identification of the value of each system and possibilities of co-sharing some of the systems with other departments in the JCPS cluster.
- Effective utilisation of data, innovation and adoption of new technologies is also crucial for SAPS. This will improve confidence in the criminal justice system institutions. The development of MySAPS mobile application has been slow and this is a project that has a potential of improving access to police services and enhancing confidence from citizens.

## 6. Programme Chain of Delivery and institutional analysis

ICT business processes in organisations are set up to improve operations. In carrying its mandate, an organisation requires a set of ICT systems to specifically improve turnaround time on production; improve product and service quality; enhance innovation efforts; and integrate overall ICT systems in the organisation to promote efficiency (Susanto, Heru, et al. 2019, p.193). The following section outlines the ICT programme chain of delivery in SAPS (figure 2). Institutional analysis, key performance related indicators and stakeholders are also provided.

### Figure 2. Programme chain of Delivery Highlights




**Inputs:** includes expenditure on ICT and personnel of the department

**Outputs:**

- Number of police stations with functional case and record systems
- Detection rate for serious crimes
- Number of SAPS operational systems maintained and supported by SITA
- Number of ICT systems maintained per year
- Detection rate for serious commercial crime-related charges
- Percentage of trial-ready case dockets for serious commercial crime-related charges

**Outcome:** Provision of ICT capability that meets the department's operational and service delivery requirements.

**Impact:** A safe and secure ICT environment that is conducive for service delivery and the department's operational needs to ensure that all people are and feel safe.

**SAPS ICT processes, institutional analysis and legislative framework**

**Table 2. Key legislative frameworks and policies related to ICT**

| Legislation/Regulations and Policies | Key provisions |
|---|---|
| ▪ Public Service Act (2001)<br>▪ Public Service Regulations (2016)<br>▪ State Information Technology Agency Amendment Act, 2002<br>▪ State Information Technology Agency General Regulations of 2005<br>▪ Guidelines governing ICT contracts and procurement<br>▪ Promotion of Access to Information Act 2 of 2000<br>▪ Electronic Communication Transaction Act<br>▪ Public Finance Management Act (PFMA) (1999)<br>▪ Treasury Regulations, 2005<br>▪ Preferential Procurement Policy Framework Act (No. 5 of 2000) | Public Service Regulations (2016) provisions:<br>- Issuing of information security standards in the public service<br>- Issuing of interoperatability standards<br>▪ Public Administration Management Act (PAMA) of 2014 provides for heads of departments to establish, maintain and monitor the ICT plan for the respective departments; and<br>▪ Section 14 of the PAMA provides for the heads of department to acquire and use ICTs in an **effective and efficient manner.**<br><br>**<u>SITA founding legislation and regulations</u>**<br>▪ Provides for establishment of SITA which is a state entity set up to improve service delivery through ICT technologies.<br>▪ In terms of its mandate, SITA procures ICT goods and services on behalf of departments, using economies of scale to reduce costs of ICT.<br>▪ SITA conducts standard certification in respect of all information technology goods or services, which are acquired by departments. |

| | |
|---|---|
| | ▪ The agency enhances government productivity through the use of ICT.<br><br>▪ SITA compiles and maintains an up-to-date inventory of all information systems of departments to serve as basis for determining duplication of information systems.<br><br>Mandatory services ('Musts')<br><br>▪ Private Telecoms Network<br>▪ Transversal Systems<br>▪ Transversal Data Processing<br>▪ Information System Security<br>▪ Disaster Recovery plan<br>▪ Certify against Standards<br><br>Non-mandatory services ('Mays')<br><br>▪ Department ICT Training<br>▪ Department System Development<br>▪ Department ICT Maintenance<br>▪ Department Data Processing<br>▪ Advisory Services<br>▪ ICT Management Services<br><br>Financial governance<br><br>Procurement of ICT goods and services in government is done in line with principles of fairness, effectiveness, efficiency, competitive bidding, value for money, and equity which are prescribed in the PFMA, Treasury Regulations and the Preferential Procurement Policy Framework.<br><br>SITA compiles and maintains an up-to-date inventory of all information systems of departments to serve as basis for determining duplication of information systems. |

The main ICT processes in SAPS can be categorised into provision, utilisation and maintenance. Each of these steps are discussed in the following paragraphs.

**Provision:** the provision of ICT hardware, software, and general IT services in SAPS is done by SITA together with external service providers. The State Information Technology Agency (SITA) is the biggest ICT stakeholder for SAPS as it influences the department's ICT decisions. In percentage terms, 67 per cent (R1.8 billion) of the department's spending on

computer services is incurred on SITA charges whilst the remaining 33 (R891 million) per cent is towards external computer service providers.

As per the SITA Act (Act 88 of 1998 as amended by Act 38 of 2002), SITA procures ICT goods and services using economies of scale to reduce the cost of ICT in government. Sections 7(6)(a)(i) and 7(6)(b) of the SITA Act also mandates SITA to set standards for information systems in government and to certify information technology goods and services for compliance against such standards. SITA is also able to offer support to departments by checking if certain ICT vendors and contractors have sufficient licencing rights.

The Public Finance Management Act (1999), Treasury Regulations and procurement Guidelines and frameworks are also important in informing ICT acquisition decisions in the department. Any non-compliance with these pieces of legislation may result in adverse findings by institutions such as the Auditor General (AG) and may also result into Parliamentary hearings. The National Treasury may also consider non-compliance with the PFMA (1999) when making budget allocation decisions.

**Utilisation:** refers to the use and implementation of ICT hardware, software and other IT related services. This role is predominantly played by SAPS. The ICT software used in the department's crime and operating systems is installed on devices and equipment at various police stations, offices, and departmental centres. Utilisation of ICT is also co-shared with departments in the Justice, Crime Prevention and Security (JCPS) Cluster. For example, the Integrated Justice System (IJS) case management system enhancements support electronic exchange of information across the criminal justice system by ensuring that each department has a case management system in place. However, enhancements need to be made to these case management systems to ensure that certain functions that are not standard are added. This is aimed at addressing some of the challenges that have been raised around case management and integration requirements within and between departments, e.g. outcome based workflows, case decision support, integration of digital evidence (between SAPS and the National Prosecuting Authority).

Utilisation of ICT in SAPS is also governed by Service Level Agreements (SLAs) signed with SITA and contracts signed with external service providers. Under the SLAs and contracts, terms and conditions of service are specified, life cycle and duration of projects are also indicated.

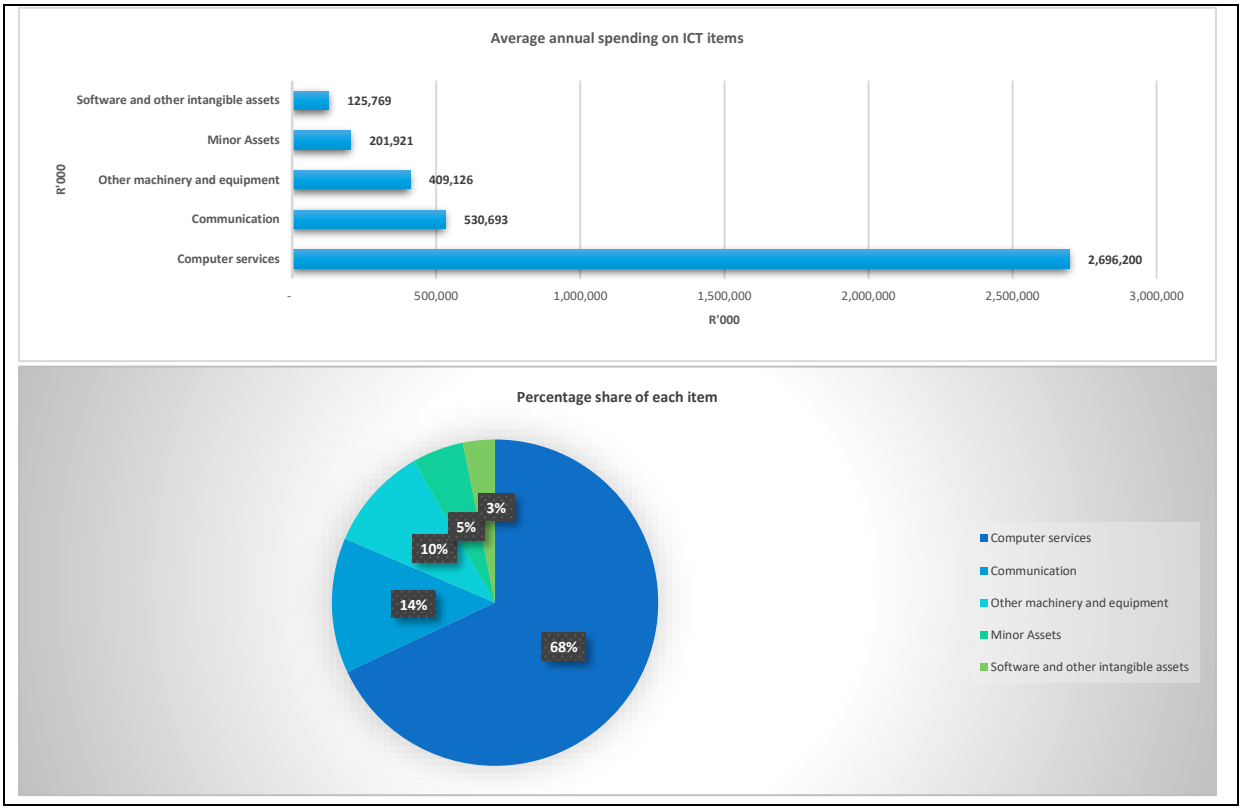
**Maintenance:** this role is mainly performed by SITA through its operational support function to SAPS. Under this function, SITA provides a fully managed operational, technical support and maintenance of applications to ensure that SAPS' applications are up to date with evolving business requirements and technology changes.

The Technology Management Services (TMS) division at SAPS Head Office is where the bulk of ICT decision making takes place. The ICT budget is also centralised within this environment. The division optimises and manages information systems and information technology for the department. In addition, the division develops and integrates information technology infrastructure (facilities and equipment) and manages applicable service-level agreements and relationships with stakeholders and service providers.

## 7. Expenditure Analysis

This section outlines the key spending drivers of ICT in SAPS. Previous sections have illustrated that SAPS spends an average of R3.8 billion per year on ICT. This spending as illustrated in figure 3 below is mainly comprised of the following items: *computer services, communication, other machinery and equipment, minor assets and software and intangible assets.*

**Figure 3. ICT cost drivers**

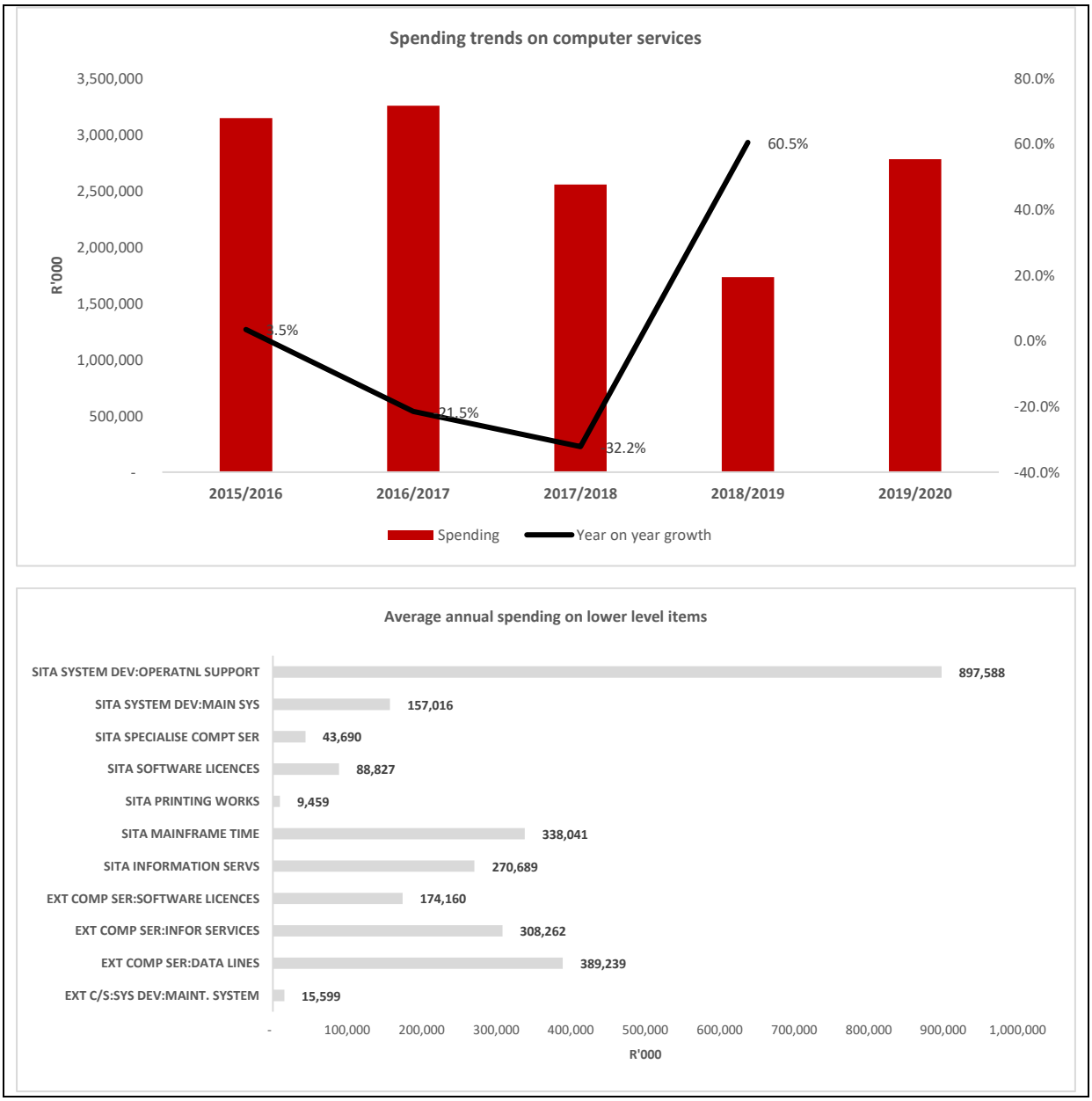



*Source: Vulindlela management information system and SAPS annual reports*

In terms of the data presented in figure 3 above, the key spending drivers of ICT in the department include *computer services* (68%), *communication* (14%), and *other machinery and equipment* (10%). Spending on *computer services* is significantly high relative to other items as the provision of ICT services, software licence fees and operational support are provided for as part of this item.

***Emerging issue 1: Spending fluctuations on computer services***

**Figure 4. Computer services lowest level items**




*Source: Vulindlela management information system and SAPS annual reports*

As reflected in figure 4 above, the key spending drivers under computer services are the following items:

**SITA system development: operational support:** this item provides for a fully managed operational support of SAPS' ICT applications to ensure they are up to date with evolving business requirements and technological changes. SAPS spends an average of R897.6 million per year for this service. Spending increases particularly between 2018/19 and 2019/20 owing to backdated payments for SITA invoices which were not finalised in the 2018/19 financial year. Flowing from the 2018/19 audit findings, the department undertook assets verification of its network and hosting sites. All sites where no orders or invoices could be found were physically inspected, and a list of the identified components which are regarded

as network assets by the department were compiled to be used to determine the fair values. This process resulted in settlement of payments to SITA during 2019/20.

**Solution:** the department needs a product and service lifecycle management strategy. The strategy will entail regular evaluation of all assets and network sites as well as ICT services. This will provide an accurate reflection of the value of all the department's assets and network sites.

SITA presented a new costing model in Parliament during 2017. The model proposed charging departments based on asset valuation, capex spending, life span of assets, direct overhead costs etc. There needs to be an alignment between the SITA costing model and invoicing of the department. This will improve stability in spending as well as promote transparency. It will also provide a cost reflective service delivery. Fast tracking the signing of service level agreements is also necessary to improve spending inefficiencies.

**SITA mainframe time:** provides a fully managed mainframe computing and application hosting service that host government applications and data in a high secure environment. Other service features include: mainframe hardware, application hosting, disaster recovery, storage, backup, data centre networking, database management systems, application platforms and systems management software.

This item represents 19 per cent of SITA charges and has recorded an average spending of R338 million between 2015/16 and 2019/20. Spending on this item grows by an average annual growth rate of 4.4 per cent which is less than inflation.

***SITA information servers***: constitute 15 per cent of SITA costs and provides for server platforms and support provision of fully managed end-user-computing and local area network services amongst others. Spending on this item shows an increase from R23 million in 2018/19 to R105.4 million in 2019/20. This is due to backdated payments for SITA invoices which were not finalised in the 2018/19 financial year. There were also several weaknesses identified on SITA's operational support to SAPS such as lack of monitoring and maintenance of the local area networks and end user devices. This resulted in disputing of invoices. Moreover, the department undertook assets verification of its network and hosting sites. All sites where no orders or invoices could be found were physically inspected, and a list of the identified components which are regarded as network assets by the department were compiled to be used to determine the fair values. This process resulted in settlement of payments to SITA during 2019/20.

**Solution:** There needs to be an alignment between the SITA costing model and invoicing of the department. This will improve stability in spending as well as promote transparency. It will also provide a cost reflective service delivery.

**SITA software licences**: represents 5 per cent of SITA charges. Spending on this item decreased from R122.4 million in 2017/18 to R12.4 million in 2019/20. Dependency on external ICT stakeholders affects spending outcomes on this item. This often results in non-compliance to prescripts relating to the payment of legitimate invoices. As such, some invoices are not finalised by the end of the financial year. Payment patterns also relate to once-off payments plus normal recurring licences paid.

**Solution:** as inefficiencies in the processing of invoices presents a business risk for SAPS, at the beginning of each financial year, the Technology Management Services (TMS) division needs to do a stakeholder and business analysis framework. This is in line with **Enterprise Efficiency modelling**. Such frameworks will provide knowledge about stakeholders, their impact on business processes of the department, outline relevant risk profiles, and history of

relations with the department. Stakeholders with bad reputation or history of non-compliance should not be used in the new financial year. For secondary ICT stakeholders (i.e. companies contracted by SITA), the department may engage SITA to ensure they comply with legislative prescripts.

In addition to the fluctuations in spending presented above, there are also inefficiencies in the supply chain management environment which have been identified in the department. In 2018/19, the department obtained a Qualified Audit opinion partly as a result of contracts entered into by SITA on behalf of the department which resulted into deviations from procurement processes, and infringement of the PFMA (1999), Treasury Regulations and the Preferential Procurement Policy Framework Act (2000) and its Regulations (2017). There were also issues raised by the Auditor General (AG) regarding lack of market analysis in SITA's pricing model. The AG also raised the issue of inaccuracies in the department's register reflecting network and hosting assets.

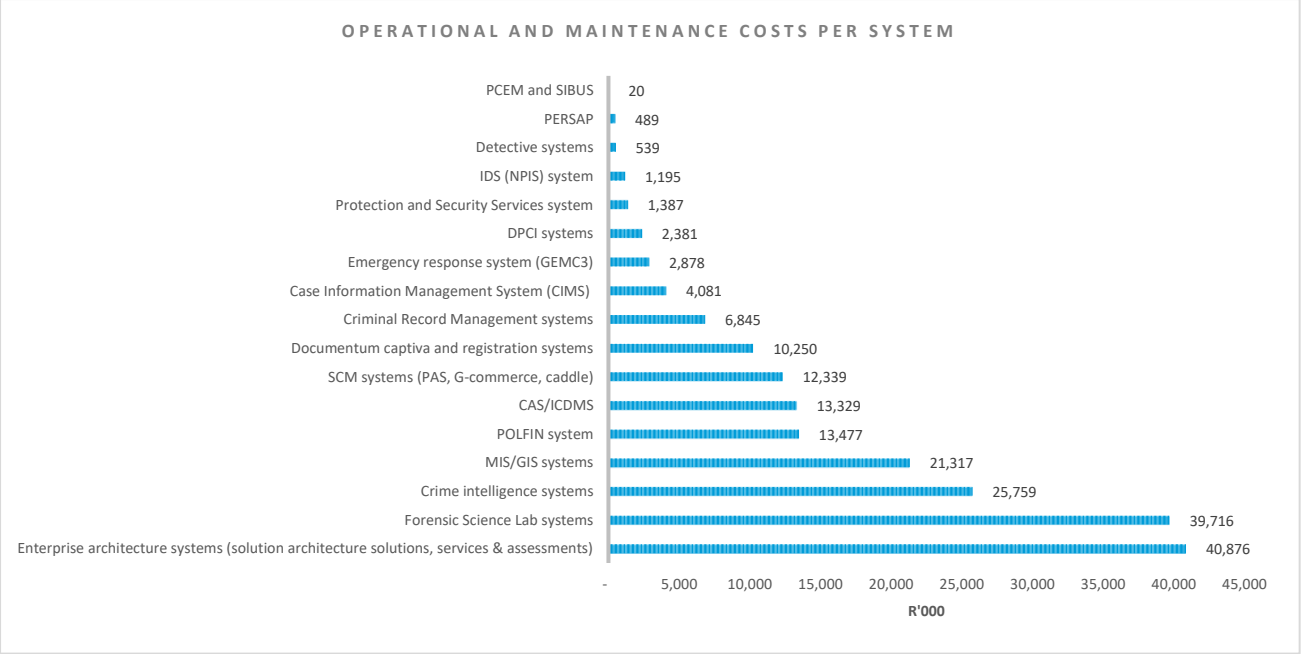
***Emerging issue 2: SITA extensive involvement in some areas increases costs and may compromise security management***

The discussion above shows that the department is also heavily dependent on SITA for several systems and the justification for such is not clear. An efficiency enterprise framework supports security management in organisations among other factors. In terms of Section 17.5 of the SITA General Regulations (2005), SAPS in concurrence with the Director-Generals of the National Treasury and the Department of Public Service and Administration (DPSA) may procure information technology goods or services directly from suppliers or through an institution other than SITA. This is applicable for the procurement of specific systems which may have safety and security conditions. Notwithstanding this provision, data obtained from SAPS reflects SITA charges in relation to software licences and maintenance in the Crime Intelligence programme. Between 2016/17 and 2018/19, the department made a total payment of R168.4 million to IBMi2 and SITA for the Analytical capabilities software. SITA's involvement in such arrangements is not clear as SAPS is enabled by legislation to source certain ICT systems directly from suppliers. Companies such as IBM are also leading in technological innovation and offer customised services. The department would therefore not need SITA's involvement. There is therefore a need to obtain further clarity from SAPS as to what informs its decision to opt for SITA services relative to other service providers outside SITA.

***Emerging issue 3: SAPS spending on ICT systems. Is the department investing in the right areas?***

In this section, an analysis of ICT systems utilised by SAPS is presented. The key question raised is whether SAPS is investing in the right areas given the strategic potential of ICT for the department. The key challenge confronting SAPS is to effectively and efficiently utilise ICT systems in a manner that will improve service delivery and promote digital transformation in the department. Figure 5 below presents a summary of ICT systems used by the department. The data presented is from 2014/15 to 2019/20.

**Figure 5. Annual average cost for operating and maintaining each ICT system (2015/16-2019/20)**

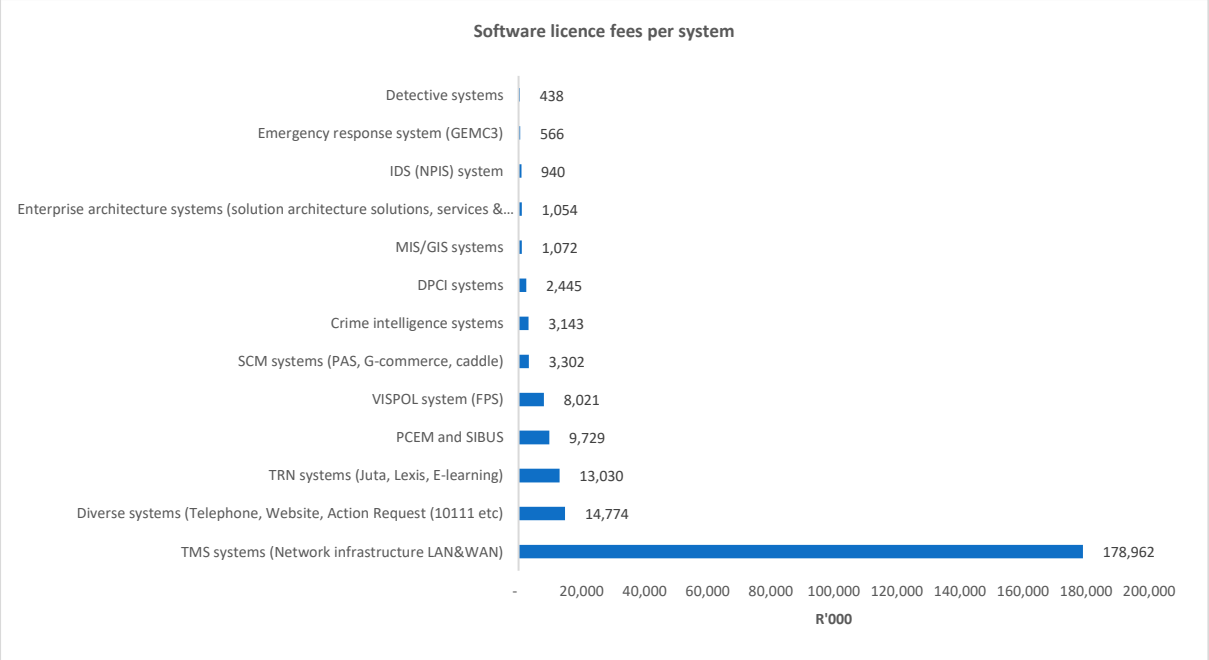



*Source: SAPS*

As presented in figure 5 above, the bulk of ICT operating and maintenance spending between 2015/16 and 2019/20 was on Enterprise Architecture systems (R40.9 million), Forensic Lab systems (R39.7 million), crime intelligence systems (R25.8 million), and Management Information systems (R21.3 million). The department incurs these costs annually to operate and maintain the systems. From the figures presented, the following issues emerge:

- Investment in some strategic priorities in the department such as *Detective Services* is low relative to other areas. For instance, the department spends more on administrative and procurement systems than on core service delivery systems. Between 2014/15 and 2019/20, an annual average of R13.5 million was spent on the POLFIN administrative system and R12.3 million on supply chain management systems. These figures are significantly higher when compared with the R2.4 million and R10.9 million spent on DPCI, criminal and case information systems.
- It is striking to see support function systems being prioritised more than high priority crime and service delivery functions. Administrative systems require additional support staff to capture invoices, transactions and pass journal entries. There are extra personnel costs involved.
- This is an area that needs the department to reconsider in the next financial year. Rather than investing on administrative systems, the department needs to enhance investment on digitisation of dockets.
- Emergency response is also receiving less attention in the department. Spending on the GEMC3 system which provides for a request (incident) management platform is only R2.9 million per annum. Low spending on this item limits the department's ability to effectively manage an incident that is lodged directly with a police official on duty at an Emergency Response Centre (ERC) or in person at a Community Service Centre.

**Figure 6. Annual average cost for software licence fees per system (2015/16-2019/20)**




*Source: SAPS*

To reduce ICT costs, organisations review systems and their relevant costs. They also identify systems that are no longer effectively utilised and change these to save costs. Systems that have reached certain life cycle must be replaced.

In figure 6, average annual costs of software licence fees per system in SAPS are presented. These fees are paid to various parties such as SITA and external ICT companies. Software licence fees are mainly high on network infrastructure systems. These systems provide for modernisation of the SAPS network and prioritised sites. This includes digital radio communication infrastructure sites and national network communication infrastructure sites. The department spends an average of R179 million on licence fees for these networks. Spending increases are linked to the number of sites upgraded and modernised. In 2019/20, 30 digital radio communication infrastructure sites were modernised. In the same year, 3 Wide Area Network (WAN) sites were modernised.

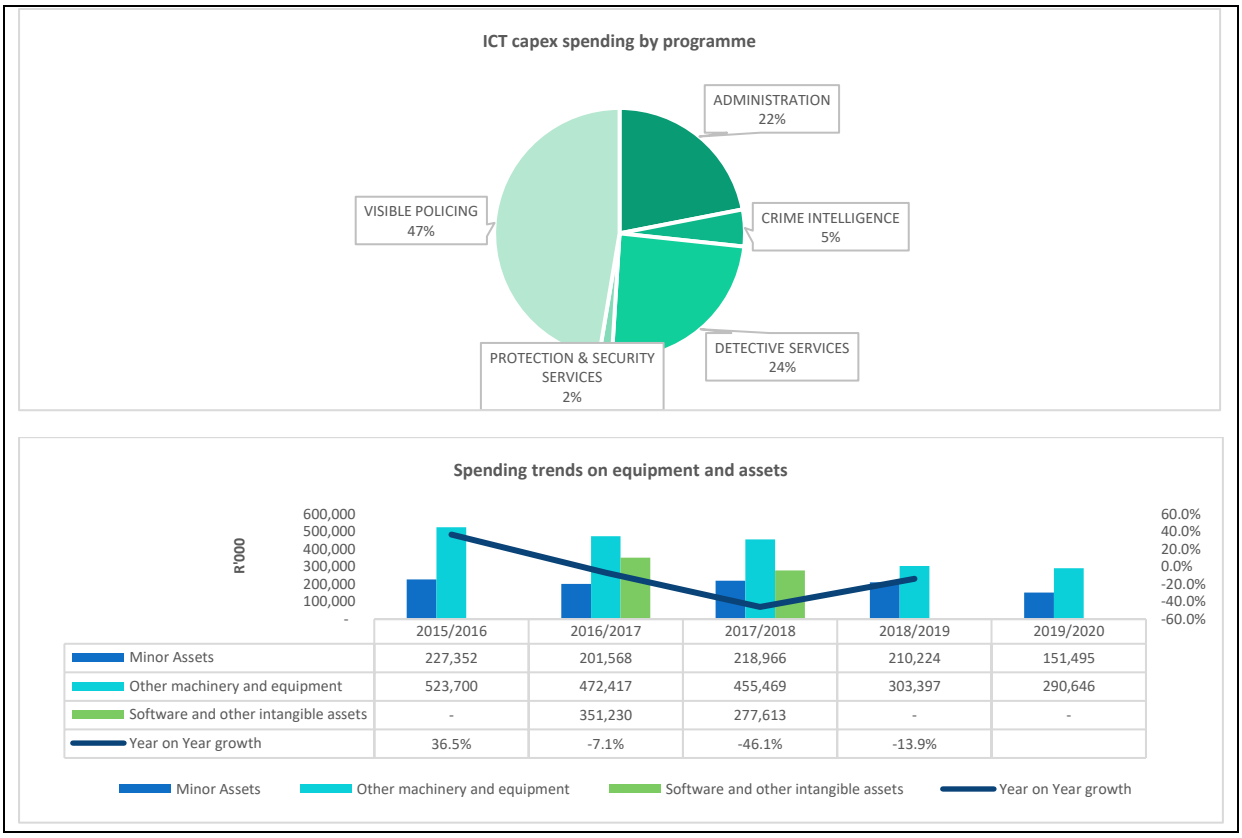
There is scope for reducing spending on some systems such as the telephone management systems particularly for support staff who are not in frontline services. This can be done through the use of virtual platforms such as Microsoft Teams for communication. The Office of the Chief Justice (OCJ) is one of the examples SAPS can learn from in this regard. The OCJ spends an annual average of R13.8 million on communication and spending on this item has been decreasing between 2016/17 and 2019/20 as a result of the OCJ implementing a unified telecommunication system (voice over internet) which is a more cost effective option than utilising landline services. This is an option SAPS can consider particularly for support function staff.

### *Emerging issue 4: Inefficiencies in spending on ICT equipment*

ICT components include a diverse set of technological tools and resources used to transmit, store, create, share or exchange information. As reflected in figure 7 below, ICT capital spending in SAPS is mainly incurred in the *Visible Policing* (47%), *Detective Services* (24%), and *Administration* (22%) programmes. This is to provide for information systems and technology to support the business objectives of the department. The key items include: cell

phones, laptops, detective equipment for crime scenes, computer hardware, radio communication devices for police officers and other minor assets.

**Figure 7. Capex spending on ICT**




| | 2015/2016 | 2016/2017 | 2017/2018 | 2018/2019 | 2019/2020 |
|---|---|---|---|---|---|
| Minor Assets | 227,352 | 201,568 | 218,966 | 210,224 | 151,495 |
| Other machinery and equipment | 523,700 | 472,417 | 455,469 | 303,397 | 290,646 |
| Software and other intangible assets | - | 351,230 | 277,613 | - | - |
| Year on Year growth | 36.5% | -7.1% | -46.1% | -13.9% | |

*Source: Vulindlela management information system and SAPS annual reports*

ICT capex spending is less than operational spending in the department. The spending trends on ICT equipment reflect a downward trend between 2015/16 and 2019/20. Year on year growth on all ICT equipment spending decreased from 36.5 per cent in 2015/16 to 14 per cent in 2019/20. Among the reasons for low spending are delays in the procurement of *Detective Services* equipment and slow implementation of the criminal justice system 7-point plan.

As a result of these delays and inefficiencies, funds are often declared unspent. In the 2018 Adjustments Budget, R150 million in unspent funds was declared on the budget for the implementation of the criminal justice system 7-point plan. This was due to projected underspending. By the end of September 2020, only R12.9 million (3%) from a budget of R440.4 million had been spent in the implementation of the integrated criminal justice strategy.

**How can SAPS address inefficiencies and poor spending on ICT equipment?**

Develop and implement clear project scope for all projects and programs related to the criminal justice system 7-point plan.

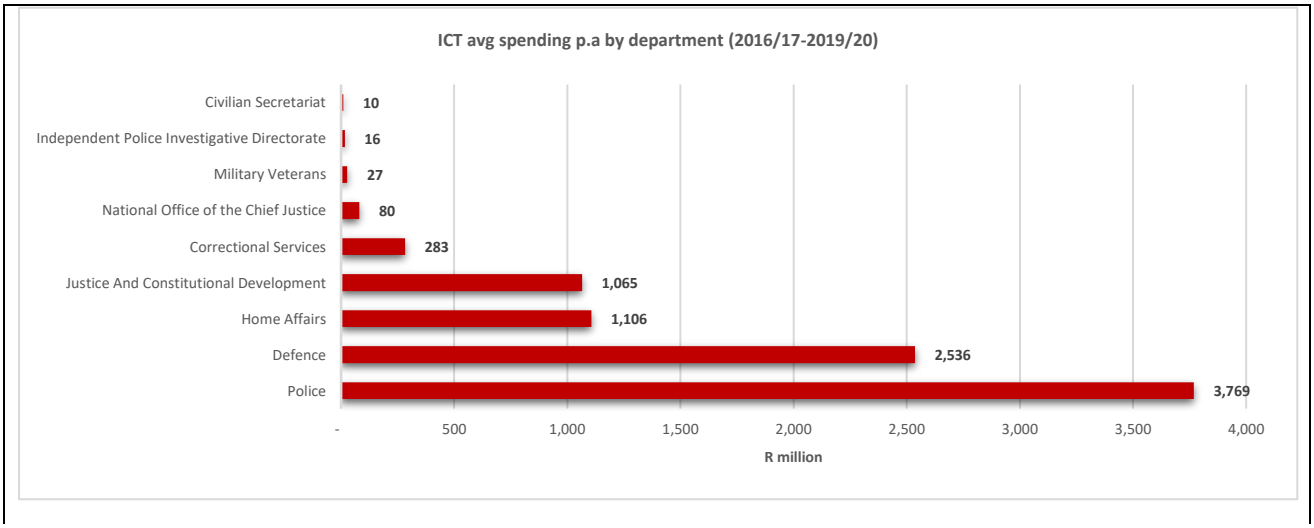
Implement Enterprise Efficiency model to improve business operations in the relevant divisions and units. This can be done by incorporating the enterprise architecture services and solutions provided to the department by Oracle. As reflected before, SAPS spends an average of R41 million per year on enterprise architecture systems and solutions. This can be better utilised in the *Detective Services* environment to address inefficiencies.

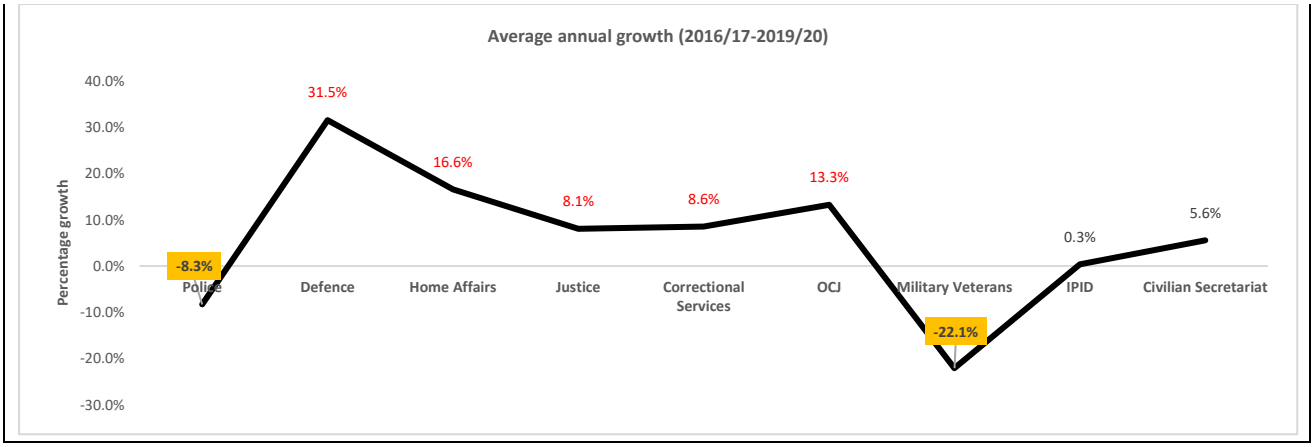
Utilisation of the SAPS IJS Repository needs to be enhanced. This service supports integration of all project knowledge bases while also providing support to organisational processes and development. It further provides for quality management, promotes the use of software to enhance technical support.

### Benchmarking of ICT costs in the Justice, Crime Prevention and Security (JCPS) Cluster

The JCPS Cluster departments utilise ICT to enhance operations and deliver services in line with their respective mandates. Most importantly, information is central in the JCPS environment hence the significant role of ICT. For instance, the police service utilises information and ICT systems to prevent and investigate crime. Institutions such as the Department of Justice and Office of the Chief Justice (OCJ) utilise information and systems to decide if an accused offender is innocent or guilty. They also decide what sentence should be given if someone is guilty. This is facilitated by availability of ICT systems across JCPS departments. The JCPS departments are also top customers for SITA services.

**Figure 8. Comparison of ICT spending per department**






*Source: BAS, annual reports and Vulindlela management information system*

In ranking ICT average spending per department between 2016/17-2019/20, the four leading institutions are: Police (R3.8 billion), Defence (R2.5 billion), Home Affairs (R1.1 billion) and Justice and Constitutional Development (R1.1 billion). Departments with the least spending on ICT include: the departments of Military Veterans (R27 million), Independent Police Investigative Directorate (IPID) (R16 million) and Civilian Secretariat for Police Service (CSPS) (R10 million). The Department of Home Affairs has been included for benchmarking purposes as it is part of the Peace and Security Function group. There is also information sharing between departments in the JCPS cluster and Home Affairs. For instance, the Automated Identification Fingerprint System (AFIS) used by SAPS interfaces with Home Affair's National Identification System (HANIS) for biometric identification of persons.

As presented in figure 8 above, relative to other departments, average annual growth rates in ICT spending between 2016/17 to 2019/20 are significantly high in Defence (32%), Home Affairs (17%), Office of the Chief Justice (13.3%), Justice (8.1%) and Correctional Services (8.6%). Spending increases on ICT in the JCPS environment are due to the development of new systems i.e. disaster recovery and electronic document systems in Defence, replacement of assets that have reached the end of their useful life; implementation of modernisation projects in departments such as Home Affairs; and meeting increasing ICT infrastructure demands when new high and low courts are established. Spending increases on software licence fees across all departments is driven by payment of Microsoft licenses in US dollars, which is affected by the rand dollar exchange rate.

***Emerging issue 5: Adopting and learning ICT best practices from Home Affairs***

**Table 3. Home Affairs: ICT case study**

| R'000 | 2016/2017 | 2017/2018 | 2018/2019 | 2019/2020 | Average spending per year | Average annual growth rate |
|---|---|---|---|---|---|---|
| COMMUNICATION | 82 623 | 49 798 | 45 317 | 39 287 | 54 256 | -21.9% |
| COMPUTER SERVICES | 581 705 | 633 397 | 575 830 | 668 877 | 614 952 | 4.8% |
| CONSULT:BUSINESS&ADVISORY SERV | 359 | - | 384 | 490 | 308 | 10.9% |
| CONTRACTORS | 7 | 300 317 | 315 509 | 254 287 | 217 530 | 3294.7% |
| MINOR ASSETS | 4 660 | 5 973 | 6 210 | 5 991 | 5 708 | 8.7% |
| OTHER MACHINERY & EQUIPMENT | 51 605 | 250 969 | 87 954 | 112 581 | 125 777 | 29.7% |
| SOFTW & OTHER INTANGIBLE ASSETS | 28 895 | 174 124 | 39 741 | 105 696 | 87 114 | 54.1% |
| **Total** | **749 852** | **1 414 579** | **1 070 945** | **1 187 208** | **1 105 646** | **16.6%** |

*Source: BAS*

The department of Home Affairs is an interesting case study as it offers possibilities of benchmarking ICT costs and transformation in government. Over the years, the department has implemented its modernisation programme which entailed rolling out smart ID cards, digitisation of records, improving business processes and technology infrastructure in the department. The programme has also assisted the department to transform its overall operations for improved service delivery.

From table 3 above, it is reflected that the department spent an annual average of R1.1 billion between 2016/17 to 2019/20 on ICT. The key spending drivers include *computer services, contractors* and *other machinery and equipment*. These items recorded average annual growth rates of 5 per cent, 3 295 per cent and 54.1 per cent, respectively. The spending increases are linked to the modernisation project which the department has been implementing in phases over the years. For instance, the department collaborated with the banking sector to roll out smart ID cards and passports to citizens, hence the significant growth in spending under *contractors*. Given the success of the programme, the department won the prestigious ICT Service Delivery Transformation Award in the National Government category for two consecutive years (2015 and 2016).

It is interesting to note that in the case of Home Affairs, computer services spending only represents an annual average of R615 million which is significantly less than that of Police (R2.6 billion), Defence (R795 million), and Justice and Constitutional Development (R707 million). This suggest the department is able to run its ICT programs/platfomrs with less SITA charges compared to other JCPS departments. However, ICT operational support in the department is still predominantly provided by SITA as mandated by legislation.

Home Affairs also presents a model that can be replicated by SAPS as Home Affairs has managed to roll out its modernisation applications across its centres in the country. On the contrary, SAPS had 1 154 police stations in 2019/20, yet only 60 (5.2%) had the automated fingerprint system (AFIS). There is therefore scope to improve digitisation initiatives in SAPS.

As SITA operational support challenges are experienced across departments, the department of Home Affairs in 2018/19 implemented an Uninterruptable Network Strategy and Investment Plan to ensure dedicated DHA network connectivity for WAN and LAN and stabilisation of the network. Given the significant costs incurred by most departments in the JCPS cluster on SITA services, there is scope for exploring the DHA strategy as it may assist in minimising operational weaknesses and system downtimes.

***Emerging issue 6: Enterprise Efficiency Framework issues that need to be addressed***

The enterprise efficiency issues that must be addressed in the department include technical issues and lack of innovation. These are discussed below.

***Technical issues and lack of innovation***

Systems in the department are not updated regularly. For instance, for financial and admin processes, the department uses POLFIN which is an old system that requires manual capturing of information. At the end of the 2019/20 financial year, the department spent R16.8 million to maintain the POLFIN system. An enterprise efficiency framework supports innovation, operational efficiencies, and integration between systems of an organisation and its stakeholders. As POLFIN is mainly an internal system of the department, it is not well integrated with other government systems such as BAS, Vulindlela and this limits transparency and creates inefficiencies in terms of internal controls.

Spending on systems development has been declining by an average annual growth rate of 0.9 per cent between 2016/17 and 2019/20. It is not clear if SITA depreciates hardware and software in the department at industry standard rates to allow for adoption of new innovations.

# 8. Performance Analysis

ICT does not only provide operational tools and administrative systems, but it also serves as a 'force multiplier' for police departments (Jackson et al. 2014), enabling the departments to use smart ways of policing. To effectively do so, ICT needs to be embedded within the operations of the department. This will support performance improvement and service delivery. The following section strives to draw the link between ICT systems used in the department and performance outcomes in various divisions such as *Detective Services* and *Crime Intelligence*.

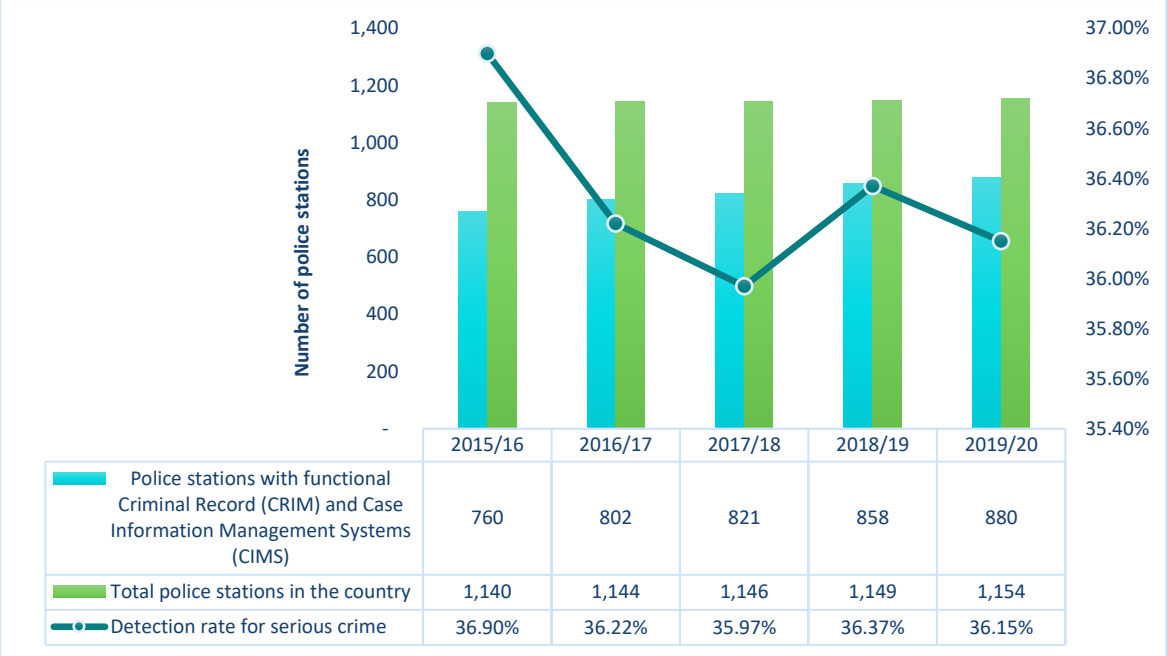
As presented in figure 9 below, the key inputs include spending information and the personnel utilising the ICT systems in the department. Outputs relate to performance indicators linked to service delivery.

**Figure 9. Systems model for performance measures**


### *7.1 Weaknesses in record management systems*

Record management is crucial in the effective investigation of serious crime (Dearstyne 2007). This is linked with effective utilisation and management of information systems used by law enforcement agencies. Yet as reflected in the department's data, only a selected number of police stations have functional case and record management systems in South Africa. This is presented in figure 10 below.

**Figure 10. Police stations with functional case investigation and record systems**




| | 2015/16 | 2016/17 | 2017/18 | 2018/19 | 2019/20 |
|---|---|---|---|---|---|
| Police stations with functional Criminal Record (CRIM) and Case Information Management Systems (CIMS) | 760 | 802 | 821 | 858 | 880 |
| Total police stations in the country | 1,140 | 1,144 | 1,146 | 1,149 | 1,154 |
| Detection rate for serious crime | 36.90% | 36.22% | 35.97% | 36.37% | 36.15% |

*Source: SAPS*

As reflected in figure 10 above, over the past five financial years, the number of police stations with functional Criminal Record Management (CRM) and the Case Information Management System (CIMS) increased from 760 in 2015/16 to 880 in 2019/20. Over the same period, the total number of police stations increased by 14, from 1 140 to 1 154. However, the detection rate for serious crime declined from 36.90 per cent to 36.15 per cent, respectively.

Despite an increasing budget allocation on ICT systems over the past 5 years, the detection rate remains low and the delays in the finalisation of investigations are also persistent. This raises a question on the effectiveness of some of the systems used by the department such as the Criminal Record Management (CRIM), Case Information Management System (CIMS) and Investigation Case Docket Management System (ICDMS). These systems were developed to provide enhanced capability to the department through the implementation of procedural workflow thus enabling investigating officers to initiate and conduct investigations in a structured, timely and cost-effective manner.

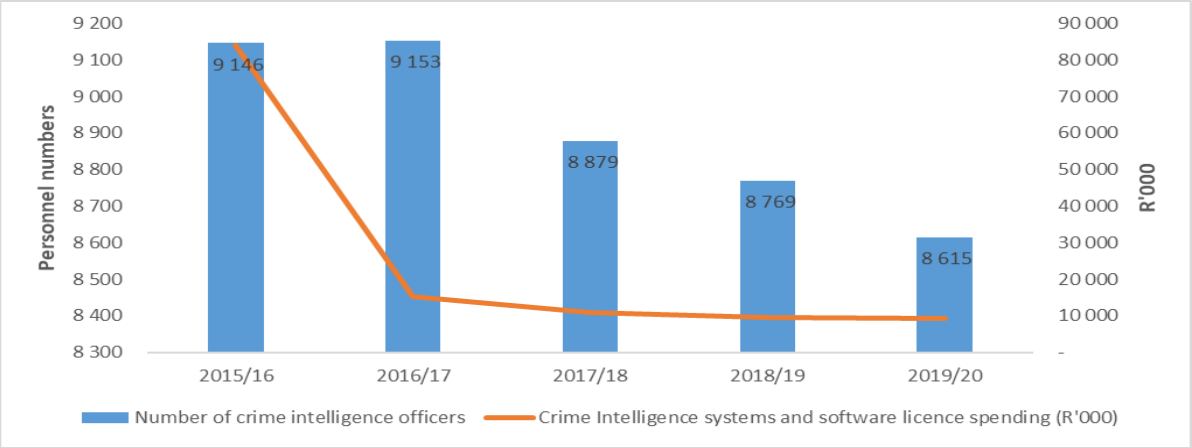
There is also mismanagement of data flow volumes reflected through case backlogs. This compromises data quality as some case dockets may get lost and limit effective processing of investigations. There are also inefficiencies in developing and implementing e-dockets systems.

These issues therefore suggest poor case flow management, inefficient record management systems, lack of detective capacity in some police stations and slow implementation of ICT modernisation in SAPS. At the end of the 2019/20 financial year, only 76.3 per cent (880) of police stations had functional case and record systems. In the same year, spending on maintenance of the CRMand the CIMS was R27.4 million. As the department incurs expenditure for software licence fees for these systems, it is not justifiable that some police stations do not have proper digital and information system arrangements.

### *7.2 Opportunities for smart and intelligence-led policing*

Smart and intelligence-led policing are key strategies of detecting and preventing crime (Ribaux et al. 2010; Ratcliffe and Guidetti 2008). The adoption of an intelligence-led policing model is essential for combatting cybercrime and in the identification of high-risk offenders (Ezeji and Olutola 2018, p.167). Intelligence-led policing is also suitable for the South African context given high contact crime rates, limited resources for appointing additional personnel in government and the need for crime deterrence in high risk areas.

**Figure 11. Crime intelligence officers vs. spending on intelligence systems**




*Source: SAPS*

As depicted in figure 11 above, SAPS has lost a significant number of crime intelligence officers. Between 2015/16 and 2019/20, the department's crime intelligence personnel decreased by 531, representing an average decrease of 133 officers per year. This also may contribute to the decline in the detection rate for serious crime. Over the same period, the department's spending on intelligence related systems also significantly declined from R84 million to R9.3 million.

Given the strategic role of crime intelligence and smart policing in national security, it is concerning that resources in the crime intelligence environment seem to be declining. The decrease in personnel is not supported by investment in technology which is essential for smart policing. Intelligence-led policing has been proven to be a 'collaborative enterprise' between law enforcement agencies and communities (Gonzales and Herraiz 2005, p.18). As such, implementation of a system for disseminating information appropriately is necessary. Research also shows that professionalisation of intelligence services is essential for creating public value and that intelligence analysis centres utilise technology to strengthen secret services oversight (Omand 2010, p.41).

For law enforcement agencies, ICT has also been identified as crucial for enhancing intelligence-led and smart policing methods as it provides tools and analytic devices that support intelligence operations. Financial and cybercrime enforcement requires ICT capabilities and innovation. Accordingly, the department needs to prioritise the intelligence environment particularly through ICT capacitation. This can be done through identification of less effective systems in the department and funds be reprioritised towards crime intelligence innovations.

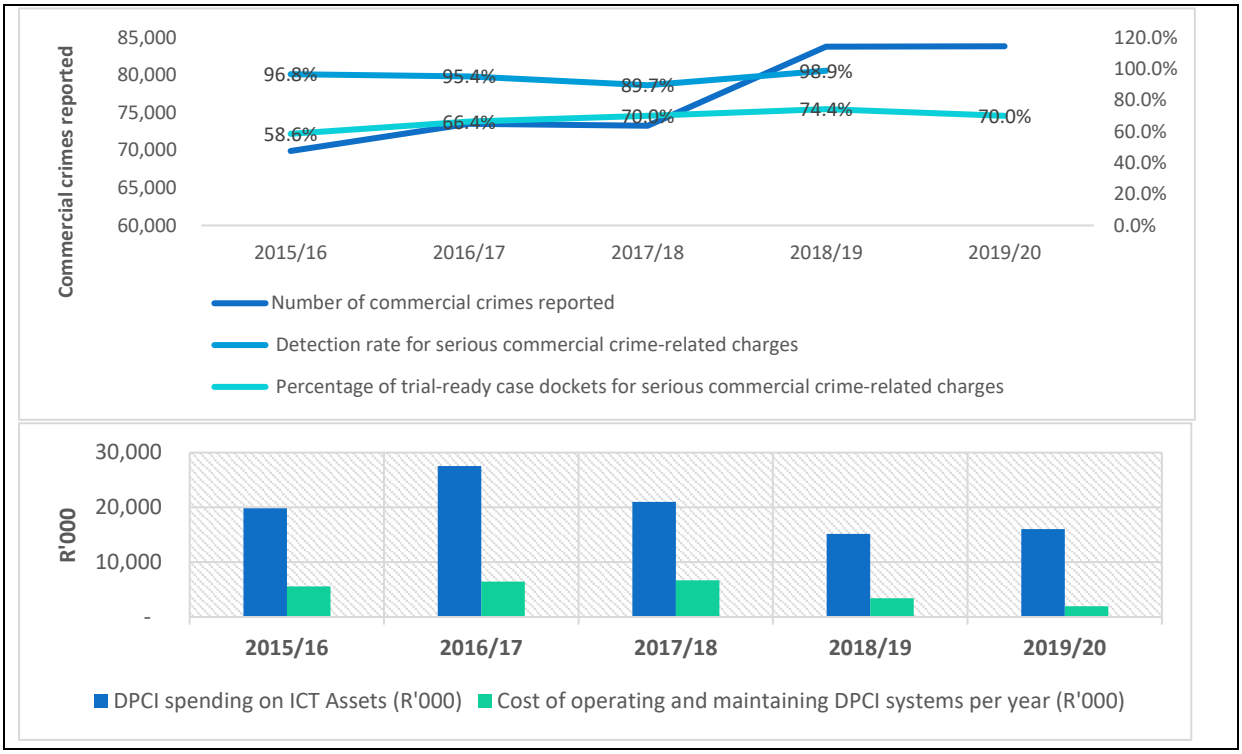
### *7.3 Priority crime investigations*

Commercial crime is classified as a serious crime and is among the highest crime categories in South Africa. Between 2015/16 and 2019/20, the number of commercial crimes reported increased from 69 917 to 83 869 which represents an average annual increase of 5 per cent.

At the end of 2019/20, commercial crimes reported were higher than other crime categories such as theft of motor vehicle and motorcycle (46 921), robbery at residential (21 130) and non-residential premises (20 651).

Figure 12 below demonstrates the important role played by specialised investigation devices and assets in the investigation processes of commercial-related crimes. These assets assist investigation officers to detect crimes such as computer fraud, money laundering, counterfeit, and fraudulent identification.

**Figure 12. DPCI ICT spending vs. performance**




*Source: SAPS and Vulindlela management information system*

As reflected in figure 12 above, spending on DPCI ICT assets has been on a declining trend particularly between 2016/17 and 2019/20. Yet, over the same period, the percentage of trial-ready case dockets for serious commercial crime-related charges improved from 66.4 per cent to 70 percent. As fraud is escalating in South Africa, the department will require additional capacity of fraud investigators which is a specialised skill set. This can be achieved through a trade-off from savings on operating systems which relative to other operating environments are less expensive under the DPCI.

## 9. Options

Based on emerging issues presented in the expenditure analysis, performance and literature review sections, the following section presents options for identifying savings, improving utilisation and efficient management of ICT in the department. The analysis thus far has demonstrated that SAPS has the potential of improving its utilisation of ICT through better adoption of the enterprise Efficiency model.

***Option 1: The department should develop and implement an Enterprise Efficiency Framework***

- SAPS spends an average of R1.7 billion on SITA costs of which R897 million is for operational support. Evidence has shown that there are multiple inefficiencies experienced with SITA particularly in terms of providing reliable and dedicated support to the department. To address this, SAPS needs to develop an enterprise efficiency framework to improve its business processes with SITA. This is in line with international best practice.
- The framework must provide a product and service lifecycle management strategy, linked to **Business systems and applications**. The strategy will also entail regular monitoring and evaluation of all assets and network sites as well as ICT services. This will provide an accurate reflection of the value of all the department's assets and network sites. The department should not pay for services where proper market related values are not provided. This will assist the department to avoid adverse audit findings.
- This can be done on an annual basis in line with asset management processes in the department.
- The framework will also address spending inefficiencies in the implementation of projects related to the integrated criminal justice system. Historical analysis has shown by mid-year, less than 50 per cent of funds are spent on these projects. Potential savings could be derived from the R809.8 million allocated in the 2021/22 and 2022/23 financial years for the implementation of the criminal justice strategy.

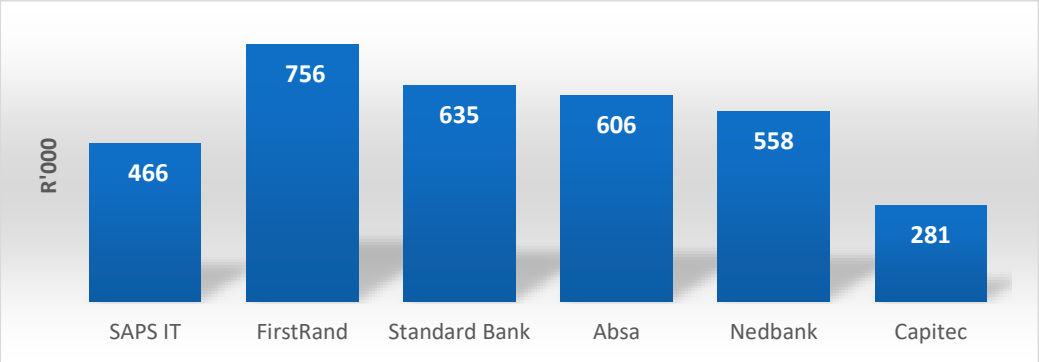
***Option 2: Digital transformation in the department will require reprioritisation of funds***

- Given the mismatch between ICT utilisation and performance in some critical areas such as *Detective Services* and *Crime Intelligence*, resources should be reprioritised from support functions. This can be done as part of the 2022 Medium Term Expenditure Framework (MTEF).
- Digital transformation will serve as an enabler for smart policing and effective investigation of high priority crimes.
- Total average cost of administrative systems is R77 million per year. Some of these funds can be reprioritised towards core service delivery ICT systems.

***Option 3: Reprioritise and invest in critical ICT skills***

Several ICT reviews discussed in the report have identified the need for governments to invest in ICT skills. Although ICT is a strategic priority in terms of its economic value chain, in many countries, ICT skills are highly concentrated in the private sector due to lucrative remuneration.

**Figure 13. Average cost per employee in SAPS IT vs. Banks (2019)**




*Source: Vulindlela management information system and Business Tech report 2019*

As reflected in figure 13 above, SAPS' IT staff are paid relatively far less than average employees in the big four financial institutions (First Rand, Standard Bank, Absa and

Nedbank). Banks such as FirstRand offer the highest remuneration to its employees and this is associated with the digital transformation and technological innovation which the institution drives. FirstRand ranks higher in the African continent in terms of technological innovation and digital banking services (Rand Merchant Bank 2020).

For SAPS to be able to implement an effective digital transformation strategy, ICT skills will need to be prioritised by the department. Reprioritisation of funds will also need to be made. The department may decide to hire specialist software developers and programmers in the Technology Management Services (TMS) environment and reduce general staff. Prioritisation of ICT skills will also reduce spending on consultants and contractors in the department.

Another option of achieving efficiency savings may be achieved through reducing the headcount numbers in the TMS division. These options are quantified

5 per cent reduction: 46 x R466 000 (R21.3 million savings per year)

10 per cent reduction: 92 x R466 000 (R42.6 million savings per year)

20 per cent reduction: 183 x R466 000 (R85.3 million per year)

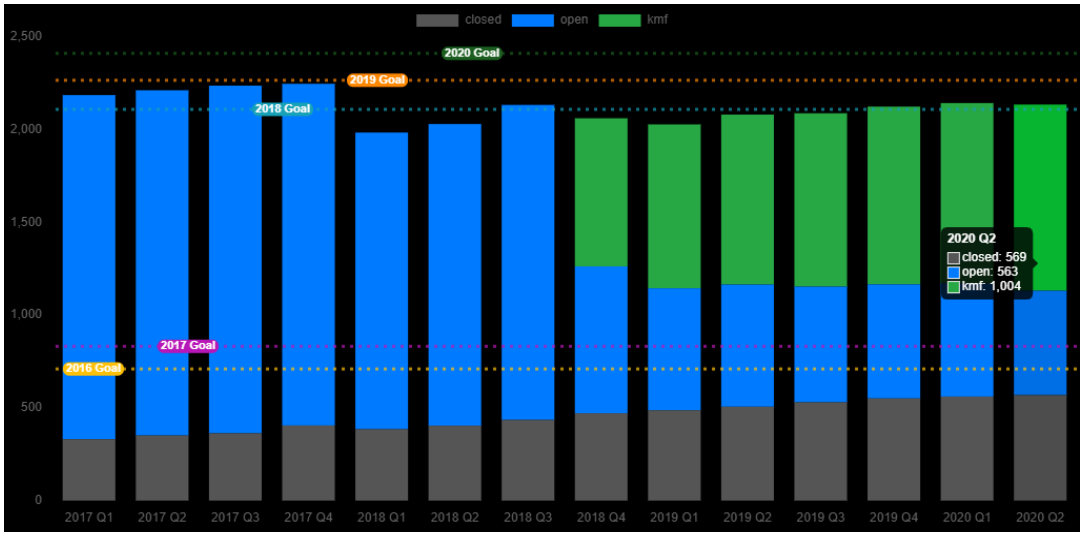
The basis of implementing headcount reductions would be to streamline the ICT function in the department and to restructure the whole TMS division to be oriented towards enterprise efficiency standards. This includes automation of business systems and applications as well as digitising services. The department will also need to test if business continuity is effectively implemented with a smaller number of staff.

Another aspect of reprioritising funds is through reducing spending on external ICT service providers. The department spends an annual average of R197 million on ICT consultants which represents almost 50 per cent of compensation spending in the TMS division. The spending on consultants is equivalent to over 300 ICT personnel in the private sector (based on average of R567 000 cost per employee in the banking sector).

***Option 4: There are cost-saving opportunities in better utilising and managing data centres/ servers***

Spending on ICT servers is among the biggest for both government departments and private companies. In 2019/20, R509.5 million was spent on SITA information and internet server charges by JCPS Cluster departments. In figure 14 below, cost saving approaches are presented.

**Figure 14. Cost savings and closures of servers in the US**




*Source: US IT Dashboard*: https://itdashboard.gov/drupal/data-center-statistics

As reflected in figure 14 above, the U.S government took a decision to optimise its data centres in an effort to generate savings, promote efficiencies and streamline ICT processes in government. All data centres that are ineffective and not being utilised have been closed. At the end of the second quarter 2020, the U.S government closed 569 centres. This initiative forms part of the Financial Lines of Business program discussed in section 3 of the report. Optimisation of data centres is a legal requirement and agencies are compelled to also declare savings from such endeavours.

Within the JCPS environment, there are opportunities of shared services and negotiating with SITA to migrate to cloud/virtual servers. This will reduce running costs, promote efficiency and collaboration among departments in the Cluster. It is for this reason that companies such as Oracle are offering innovative solutions of reducing inefficiencies.

At the end of the 2019/20 financial year, departments in the JCPS Cluster spent R771.6 million on servers. As these are significant costs, the options below will require departments to identify servers and data centres which consume significant data and storage and those that can be closed down and co-shared with other departments. It is important to emphasise this is a long-term process and has several risks. As such, efficiency savings targets need to be set as minimum as possible. From the total costs of R771.6 million, savings would be as follows:

5 per cent for departments with establishments of less than 500 employees (i.e. IPID, CSPS, Military Veterans): R38.6 million per year.

10 per cent for departments with establishments of more than 500 employees: R77.2 million per year.

***Option 5: other efficiency savings***

- Other savings may be realised through allowing the department to source systems directly from ICT service providers as per SITA Regulations. This will reduce the annual software licence fees paid to SITA which amount to an average of R88.8 million per year.
- Reducing communication can be achieved by adopting some of the best practices from the JCPS departments such as OCJ. SAPS spends an average of R530.7 million on communication of which almost 80 per cent is spent on telephone/fax/telegrap&telex. OCJ spends an annual average of R13.8 million on communication with a staff establishment of 1 989. This is as a results of the OCJ implementing a unified

telecommunication system (voice over internet) which is a more cost effective option than utilising landline services. This is an option SAPS can consider particularly for support function staff and divisions at Head Office.

**Table 4. Total savings**

| Item | Savings per year | Total savings over the MTEF |
|---|---|---|
| i) Reprioritisation of funds for the development and implementation of an Enterprise Efficiency Framework | R266 million | R800 million |
| ii) Reprioritisation of funds from administrative systems to fund digital transformation | R25.6 million | R77 million |
| iii) Reprioritisation of funds for critical ICT skills in the department | R150 million | R450 million |
| iv) Reducing spending on ICT servers through | R77.2 million | R231.6 million |
| v) Efficiency savings from communication systems | R102.8 million | R308.4 million |
| **Total** | **R621.6 million** | **R1.9 billion** |

## 10. Recommendations

1. In terms of Section 17.5 of the SITA General Regulations (2005), SAPS in concurrence with the Director Generals of the National Treasury and the Department of Public Service and Administration (DPSA) may procure information technology goods or services directly from suppliers or through an institution other than SITA. In light of this provision, the department should utilise external ICT service providers where necessary in order to identify savings.

2. The department needs to improve business operations in certain divisions such as Detective Services. Spending on ICT equipment is poor in this environment and this affects effective implementation of the criminal justice system 7-point plan. Inefficiencies can be addressed by incorporating certain aspects of the enterprise architecture services and solutions provided to the department by Oracle.

3. Information servers are a significant cost driver in the JCPS Cluster. There are opportunities for shared services and negotiating with SITA to migrate to cloud/virtual servers. This will reduce running costs, promote efficiency and collaboration among departments in the Cluster.

4. The department needs to identify ICT systems that are due to reach the end of their useful life. These systems must either be replaced or modified. This will save costs and improve internal controls.

5. SAPS can adopt some possible lessons from the Banking Sector which has lucrative remuneration structure for ICT staff who develop and maintain applications. Banks also have advanced tech systems and applications that promote innovation and cyber security.

6. Research shows that reducing IT costs is possible but requires extensive consultation and collaboration among government institutions. Within the JCPS Cluster, there is room for identification of cost-sharing arrangements particularly on financial and security systems. This approach allowed the U.S to realise massive savings and improved data quality and policy decisions.

7. Investment on ICT over the past financial years has not been met with improvements in core performance areas such as Detective Services. As such, the department must prioritise modernisation and integration of systems at police station level.

8. The department should review the value of all its ICT systems, specify their life cycles and utilise enterprise architecture frameworks to streamline its processes.

9. Similar to the Central Supplier Database, across government, there needs to be an IT Dashboard website to publish cost savings, ICT systems and relevant providers in each government institutions. This will promote transparency, allow for public scrutiny and generate savings for government.

10. Finding and using an appropriate methodology for the study was challenging. Future research may consider using semi-structured interviews or surveys to improve data collection and provide better results.

## 11. Actions

**Table 5. Actions to implement and bureaucratise recommendations**

| Recommendation | Required Action(s) | Responsible department/person | Timeline |
|---|---|---|---|
| **Review and evaluation of ICT systems in the department** | • Consultation with SITA for legitimacy and support<br>• The department must be clear on what it seeks to achieve from | SAPS and SITA | Can be initiated in the 2021/22 financial year |

| | | | |
|---|---|---|---|
| | evaluating its systems by doing an ICT cost benefit analysis<br>• Consultation with JCPS cluster departments to explore options of co-sharing and integrating systems<br>• The review of ICT systems will be helpful for the identification of synergies and potential savings in the JCPS cluster | | |
| **Improving modernisation and integration of systems at police station level and main divisions of SAPS** | • Identification of barriers and blockages limiting utilisation of ICT at police stations and main divisions<br>• Aligning utilisation of ICT with operational goals and capabilities<br>• Collaborating with other institutions in government i.e. Home Affairs<br>• Working with ICT stakeholders such as Oracle to improve operational processes and innovations | SAPS TMS and other main divisions, Home Affairs and JCPS departments | Can be initiated in the 2021/22 financial year |
| **Reprioritisation of funds within ICT systems in the department** | • Analysis of ICT requirements per division and operational environment | SAPS TMS and other main divisions | Can be implemented during the 2022 Medium Term Expenditure |

| | | | |
|---|---|---|---|
| | • Reprioritise funds from areas where ICT is under utilised<br>• SITA may be consulted for reviewing Service Level Agreements (SLAs) | | Framework (MTEF) process. |
| **Implementation of smart policing** | • Improving utilisation of ICT in critical areas such as crime and intelligence and priority crime investigating units | SAPS Visible Policing, Detective Services and Crime Intelligence divisions | Can be initiated in the 2021/22 financial year |
| **Implementing ICT best practices from banking sector and other institutions** | • Review staff establishment of the Technology Management Services (TMS) division<br>• Conduct ICT skills audit in the department<br>• Explore options of reprioritising funds for the appointment of ICT specialists to improve operational efficiency | SAPS TMS division | Can be implemented over the medium term |

## Bibliography


Albrecht, J.F and Das, D.K 2011, *Effective Crime Reduction Strategies: International Perspectives*, Taylor and Francis Group, New York.

Argyrous, G 2009, *Evidence for Policy and Decision Making,* University of New South Wales Press, Australia.

Australia and New Zealand School of Government (ANZSOG) 2008, 'Realising the benefits of investment in Information and Communication Technology', [Online], Accessed 19 September 2020, Available: <https://www.anzsog.edu.au/resource-library/case-library>.

Australia and New Zealand School of Government (ANZSOG) 2009, 'Cutting IT costs by consolidating systems: the US "Lines of Business" project', [Online], Accessed 19 September 2020, Available:

<https://www.anzsog.edu.au/resource-library/case-library>.

Bayens, G.J and Roberson, C 2010, *Criminal Justice Research Methods: Theory and Practice*, Second Edition, Taylor and Francis Group, United States.

Belvedere, V and Grando, A 2017, 'ICT-enabled time performance: an investigation of value creation mechanisms', *Production Planning & Control*, Vol. 28, No. 1, pp. 75-88.

Biryukova, O.V and Matiukhina, A.I 2019, 'ICT Services Trade in the BRICS Countries: Special and Common Features', *Journal of the Knowledge Economy,* Vol. 10, pp. 1080-1097.

Bitounis, L and Price J 2019, *Technology and National Security,* The Aspen Institute, Washington.

Campbell, G.K 2015, *Measuring and Communicating Security's Value: A Compendium of Metrics for Enterprise Protection,* Elsevier, Netherlands.

Chan, J.B. 2001, 'The technological game: how information technology is transformation police practice', *Criminal Justice,* Vol. 1, No. 2, pp. 139-159.

Congressional Research Service 2010, 'OMB's Financial Management Line of Business Initiative: A Brief Overview', [Online], Accessed 19 September 2020, Available: <https://www.everycrsreport.com/files/20100520_RL33765_47258da62a088967da9b2057d3f39e15cc18e58a.pdf>.

Dearstyne, B 2007, 'Why Records Management Matters', *Public Management*; Vol. 89, No. 10, pp. 24-27.

Deloitte 2020, 'Australia's Digital Pulse: Unlocking the potential of technology workforce', [Online], Accessed 19 September 2020, Available: <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-economics-australias-digital-pulse-2020-180820.pdf>.

Dialsingh, I 2007, 'Information Technology and the Criminal Justice System', *Crime Prevention and Community Safety*, Vol. 9, No. 3, pp. 222-223.

Ezeji, C.L, Olutola, A.A 2018, 'The use of Intelligence-led Policing in Combating Technology-based Crimes in South Africa', *Journal of African Foreign Affairs*; Vol. 5, No. 2, pp. 167-188.

Federico, I 2009, 'Digitising criminal justice in England and Wales: revisiting information-growth dynamics', *Transforming Government: People, Process and Policy*, Vol. 3 No. 1, pp. 50-64.

Gonzales, A.R and Schoefield, R.B 'Intelligence-Led Policing: The New Intelligence Architecture', [Online], Accessed 23 September 2020, Available: <https://www.ncjrs.gov/pdffiles1/bja/210681.pdf>.

Government of Australia 2008, 'Review of the Australian government's use of information and communication technology', [Online], Accessed 19 September 2020,

Available: <https://www.dphu.org/uploads/attachements/books/books_2668_0.pdf>.

Government of Western Australia 2018, 'Implementation of Government Next Program', *Office of the Auditor General,* [Online], Accessed 11 September 2020, Available:

<https://audit.wa.gov.au/wp-content/uploads/2018/08/report2018_3-GovNext.pdf>.

Jackson, B.A, Greenfield, V.A Morral, A.R and Hollywood, J.S 2014, 'Police Department Investments in Information Technology Systems', [Online], Accessed 13 August 2020, Available:

<https://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR569/RAND_RR569.pdf>.

Newcomer K.E, et al. 2015, *Handbook of Practical Program Evaluation*, John Wiley and Sons, United Kingdom.

OECD 2017, 'Benchmarking Digital Government Strategies in MENA Countries', *OECD Digital Government Studies*, OECD Publishing, Paris.

Available: <https://www.oecd.org/mena/governance/digital-governance-mena.pdf>.

OECD 2017, 'Government at a Glance 2017', *OECD Digital Government Studies*, OECD Publishing, Paris. Available:

<https://www.oecd-ilibrary.org/governance/government-at-a-glance-2017/spending-review_gov_glance-2017-42-en>.

Office of Management and Budget 2017, ‘E-Government Act Implementation’, [Online], Accessed 19 September 2020, Available:

<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/egov/documents/omb-fy-2016-egov-act-report.pdf>.

Omand, D 2010, *Securing the State,* Hurst &Co, London.

Oracle Financial Services Software Limited 2020, ‘Annual Report 2019/20’, [Online], Accessed 24 September 2020, Available:

<https://www.oracle.com/a/ocom/docs/industries/financial-services/ofss-annual-report-2019-20.pdf>.

Ratcliffe, J.H and Guidetti, R 2008, ‘State police investigative structure and the adoption of intelligence-led policing, *Policing*, Vol. 31, No. 1, pp. 109-128.

Rand Merchant Bank 2020, ‘Where to invest in Africa’, [Online], Accessed 22 September 2020,

Available: <https://www.rmb.co.za/files/pdf/Where_to_Invest_in_Africa_2020.pdf >.

Ribaux, Olivier; Baylon, Amélie; Roux, Claude; Delémont, Olivier; Lock, Eric; et al. 2010, ‘Intelligence-led crime scene processing’, *Forensic Science International*, Vol. 195, No. 1, pp. 10-16.

Sørensen, F.L 2020, *Enterprise Architecture and Service-Oriented Architecture*, Nova Science publishers, New York.

South African Police Service (SAPS) 2019, *Annual Report 2018-19,* [Online], Accessed 31 July 2020, Available: <www.saps.gov.za>.

State Information Technology Agency (SITA) 2019, *Annual Report 2018-19,* [Online], Accessed 11 August 2020, Available: <www.sita.gov.za>.

State Information Technology Agency (SITA) 2020, *Strategic Plan 2020-2024,* [Online], Accessed 11 August 2020, Available: <www.sita.gov.za>.

Strom, K 2016, ‘Research on the Impact of Technology on Policing Strategy in the 21st Century’, *National Criminal Justice Reference Centre,* [Online], Accessed 8 August 2020, Available:

<https://www.ncjrs.gov/pdffiles1/nij/grants/251140.pdf>.

Susanto, Heru, et al. 2019, *Business Process Reengineering: An ICT Approach*, Apple Academic Press, United States.

UNESCO 2006, *Using ICT to develop literacy*, UNESCO Publishing, Bangkok.

Vogt, G, Dashja, E, and Birov, S 2016, ‘Cost-Benefit Analysis of ICT-enabled Services’, *Empirica,* Vol. 1, pp.2-79.

White, S.K 2018, ‘What is enterprise architecture? A framework for transformation’, 16 October, [CIO Online edition], Accessed on 24 September 2020,

Available: <https://www.cio.com/article/3313657/what-is-enterprise-architecture-a-framework-for-transformation.html>.

World Bank 2020, ‘Trading for development’, [Online], Accessed 23 September 2020, Available:

<http://documents1.worldbank.org/curated/en/310211570690546749/pdf/World-Development-Report-2020-Trading-for-Development-in-the-Age-of-Global-Value-Chains.pdf>.