ROLE OF SAI IN PROMOTING AND AUDIT OF IT SECURITY

Compiled by: Information Technology Audit Team

SAI SAMOA

Contents

[1. Background 3](#_Toc4508027)

[2. Government ICT Initiatives 3](#_Toc4508028)

[3. Roles of SAIs in Local Government 4](#_Toc4508029)

[4. Situational Analysis 5](#_Toc4508030)

[5. Role of Information Technology Audit in Samoa 6](#_Toc4508031)

[6. What do we currently do? 8](#_Toc4508032)

[7. Road ahead from SAI Samoa 14](#_Toc4508033)

[8. Why now? 15](#_Toc4508034)

[9. What can WGITA do? 15](#_Toc4508035)

[10. Conclusion 16](#_Toc4508036)

[11. APPENDIX: 17](#_Toc4508037)

# Background

Supreme Audit Institutions (SAIs) in respective countries is in the forefront of efforts to strengthen good governance and gain public trust in government departments. The role of SAIs is evolving and more recently, even in the pacific region with the rapid increases in the use of information technology as enablers of business processes and functions.

Information technology (IT) audits are slowly becoming an audit practice for the future. The increase in the use of technology in Samoa and the accessibility to cheaper internet services foresees a rise in IT audits in the coming years. SAI Samoa is an active member of the Pacific Association of Supreme Audit Institution (PASAI). Although it is a small island nation in the middle of the Pacific, the waves of technology has reached our shores.

As Samoa and the world move towards technology enabled solutions and/or as the use of technology becomes increasingly popular in this modern age, it becomes crucial for SAIs around the world to build and develop staff capabilities in auditing electronic data, systems and processes and deploy (where necessary) appropriate data analytic tools and system security tools to be used by its staff. This is further encouraged by international standards on auditing where auditors are required to consider impacts, risks and effectiveness of both manual and computerized controls amongst many other aspects of auditing.

This paper will specifically focus on the Role of SAIs in promoting and auditing of IT Security.

# Government ICT Initiatives

In the past 3-5 years, the Government of Samoa (GoS) initiated a project to improve regional connectivity and access to the internet through support from various donors. This was part of Government reforms to improve regional connectivity and collaboration and use of information communication technologies and its long term goals to move towards a knowledge-based economy.

After years of consultations and strategizing, the government believes that the public service is ready for the ‘digital age’ recognizing the vision of a ‘professional and competent public administration that provides quality, efficient and transparent services for its citizens’[[1]](#footnote-1). The Minister of Communications and Information Technology (MCIT) is spearheading the development of cable to improve internet and services to citizens and is supported by the Prime Minister and cabinet.

In June 2018, the GoS hosted a regional conference called a Digital Pacific 2018 to discuss successes, failures, trials and tribulations in the digital realm from across the region and the world. Following this regional conference a Digital Samoa national conference 2018 was held to discuss the way forward for the country.

The outcomes of this conference revealed plans to reassess whole of government’s legislative framework, regulations, policies and systems pertaining to digital transformation, empowerment of Public Private Partnerships (PPPs) and the development of talent and digital capacity across all government sectors in response for future employments and delivery of digital services[[2]](#footnote-2). This event followed the launch of the governments Cyber Security Strategy 2016-2021 in February 2017 where online security and safety became a priority.

# Roles of SAIs in Local Government

The role SAIs play in each government differs depending on local environments however a key aspect of the functions of SAI is emphasized in ISSAI12: Values and Benefits of SAI: making a difference in the lives of citizens. This paper is written with this standard in mind and a closer look at ITA.

As government auditors we are uniquely positioned in our respective countries to contribute to public finance management. As government auditors, the values of our services are seen with the developments of our countries. We are sanctioned by our communities. Our people and communities have placed their trust on us as professionals in our field to provide them with credible and high quality reports. “

Today, it is our duty not only to provide broadband access and affordable I.C.T. services for all, but also to put I.C.T. at the service of other economic sectors such as health, education, agriculture and trade’

*Source: Statement by the Minister of MCIT in their 2017 Annual Report*

In today’s world, becoming a government auditor comes with a number of challenges. As government auditors we need to continuously grow in our field and adapt our practices to changes as they occur. The core role of SAIs through public sector auditing is making a difference in the lives of citizens. There is a public expectation for government auditors to provide assurance on accountability, transparency and integrity of government and public sector entities made out as an opinion on the truth and fairness of financial statements and/or an audit conclusion as to the effectiveness and efficiency in the use of public funds. This places SAIs as a credible source of independent and objective insight, supporting beneficial change in the public sector.

The auditor's specific audit objectives do not change whether accounting data is processed manually or by computer. This follows and observes the Samoan age old concept that principles and foundations will remain, but practices do change in accordance with the circumstances of the day (PASAI Newsletter; CAG Samoa). The auditors can use either manual audit procedures, computer-assisted audit techniques, or a combination of both to obtain sufficient evidence on a subject matter.

# Situational Analysis

Prior to the Samoa Audit Office Institutional Strengthening Project (ISP), there was little to no recorded knowledge of any technical IT auditing activities being carried out within Samoa due to the lack of available IT audit skills within the country and high costs associated with engaging overseas experts in this area. For a small island, with very limited resources the demand for such skills and knowledge were trivial compared to the demands and needs of the health, education and infrastructure sectors.

On a country-wide scale at the time of the ISP it was found that there was a general lack of IT skills within Samoa - where a typical ministry or public body is considered fortunate if they employ more than one IT qualified professional. During this time, many controls considered fundamental in larger organizations overseas, such as strong segregation of duties between IT staff and accountants and even within the IT area were generally not very prevalent within Samoa.

At the end of the ISP, a comprehensive IT audit manual and methodology was developed and documented. This methodology covered all stages of the IT Audit process from strategic planning, detailed execution, documentation, reporting and follow up. It was sourced from a number of existing best practice guides including ISACA materials, IT Audit Manuals from SAI India and other materials from various audit offices in Australia. All nominated IT Audit staff were trained in the IT Audit Manual and Methodology, and SAI Samoa’s leadership group were trained in an overview of the methodology and in particular how it links with the financial audit process.

Since the establishment of ITA in 2010 and government reforms in areas of Information and Communication Technology (ICT) gradual improvements was seen across the public sector. SAI Samoa is in its fifth year of its ten-year Strategic Plan. One of the main goals of this Strategic plan is **‘the improvement of quality, efficiency and timeliness of audits’**. To achieve this goal we felt it necessary to analyze the current position of ITA within our office. The result of this assessment is tabulated in Appendix One. SAI Samoa has come a long ways with developing ITA capabilities within the office and has continued to grow within the SAI.

Whilst computer (s) may be involved in producing financial statements, the overall objective of a financial audit does not change

 **To provide an “audit opinion”**

# Role of Information Technology Audit in Samoa

An IT Audit as defined is **any audit involving the examination of automated information processing systems; related manual and non-automated processes; and interfaces between automated & non-automated processing systems.** It is not limited to just examining IT system components, such as hardware and software but encompasses of the assessments of any related manual controls and procedures.

The SAI Samoa is empowered under Section 46 of the Audit Act 2013 to conduct ITA where the CAG may:

Traditionally, the role of IT audit was primarily focused on supporting financial audit. The scope of work performed was generally limited to work associated with financial statements. This was a result of concerns to auditors about the reliability of data within computerized systems particularly as most audit trails are electronic.

**TABLE 1: ITA Methodology**

Financial Statements

Application Controls

IT General Controls

**Trial Balance Data**

With the above diagram in mind, the following is generally considered for our financial audit support for the various layers depicted in Table 1:

|  |  |  |
| --- | --- | --- |
| Hardware Layer | Operating System Layer | Application Software Layer |
| Uncontrolled access to computer hardware can result in the following risks | Personnel with operating system super-user security access rights have:- | Unauthorized creation, alteration or deletion of transactions and master file data. For example:- |
| * theft of, or damage to, physical computer assets
* unauthorized access to backup tapes/disks
* unauthorized use of disk utilities to read or alter data or disks
* introduction of computer viruses onto servers - via memory sticks
* leakage of confidential data (e.g. customer lists, supplier discount structures etc.)
 | * the means to alter and/or delete all data, files and programs on the system, from which the trail balance data and financial statements are derived
* the ability to start and stop the computer system
* run (or stop) any program (from running)
* alter or delete entire databases and system interface files
* delete all system log files
 | * adding fictitious employees,
* altering a debtor balances by fictitious credit notes; and
* unauthorized debtor write-off transactions
* creation of invalid accounting period end dates
* override controls over 3 way matching between purchase orders, delivery and supplier invoice controls
 |
| **Each layer in the pyramid introduces new levels of risks to a financial auditor, charged with expressing an opinion on the financial statements.** |

In more recent years and further exposure to International Standard for SAIs (ISSAIs), SAI Samoa has been progressing towards more performance based audit engagements. There is no question about whether or not SAI require dedicated and well trained auditors in the areas of ICT.

There is now a growing need for SAIs to be capable of competently reviewing computerized accounting systems and supporting I.T. infrastructure used across the public sector. Additionally, a thorough understanding of business and control risks associated with computerized systems is required, in order to effectively audit today’s business systems. IT auditors are often used to evaluate the reliability of computer generated data that supports financial statements and the adequacy of controls within and surrounding information systems.

# What do we currently do?

SAI Samoa has come a long way in terms of capacity building programs. The never-ending efforts of the CAG have seen great improvements in establishing strong foundation on which the service of the SAI is based. This include relevant amendments to SAI Samoa’s enabling legislation which enforced the establishment of ITA Unit, various means of capacity building which empowered the completion of ITAs and the increase use of IT infrastructure within the Office.

Over this period, our office has managed to automate **support work** for our Financial Audit team. This comprises of data analysis for specific business cycles which offers great support to our financial auditors. This has also improved the timeliness and quality of audits completed. In saying that, most of the work conducted by our ITA team focused on providing useful data analysis to support the needs of our Financial Audit.

**The prime role of the SAO IT Auditor is to provide “expert” advice to Financial Audit in order for them to assess I.T inherent and control risks and the most appropriate audit procedures to perform, in forming an audit opinion.**

The following process is snapshot of the work performed by the ITA within SAI Samoa:

The responses from IT Inventory Questionnaire and IT General Control (ITGC) reviews are used to update Client’s IT Risk Assessment categorizing clients into high, medium or low risk clients for ITA purposes and reviews. Ideally the IT Risk Assessment would determine the level of work ITA will conduct for a specific client and also its involvement in an audit engagement.

Information system or IT controls are generally classified into two major categories and this forms the core functions of ITA within SAI Samoa which aligns with available guidance on ITA including ISSAI5300: Guidelines to ITA and ISSAI1315: Identifying and assessing the risks of material misstatements through understanding the Entity and its Environment.

**USE OF ITGC REVIEW TO ASSESS IT SECURITY:**

A common definition of ITGC reviews is that is provides an overview of the IT governance within the clients. The main objective of these reviews as is to assess the surrounding IT environment which apply to all systems, components, processes, and data present with an organization.

As auditors, our main concern is with the appropriate implementation of systems, the integrity of programs and data files and effectiveness of computer operations and its alignment with business goals, objectives and strategies. As such, our reviews are guided by three key principles which are commonly promoted in the field of ICT; these being confidentiality, integrity and availability.

The reviews are usually conducted in a form of a questionnaire (issued via free online services specifically Google forms) to obtain information about the design and governance of ITGC and survey questions focus on obtaining an understanding about policies, procedures and processes surrounding IT environment. The responses from these questions are evaluated by the team and further discussed with the client’s IT Managers to arrive at a conclusion on the design and operational effectiveness of controls based on best practice guides. This will also determine where the IT Control processes can be relied upon and findings are usually presented as a standalone audit report.

The most common areas assessed by our Office include:-

1. IT management controls – IT Strategy, Organizational Structure and Security Policies (antivirus controls, internet and email use, etc)
2. Physical/environmental security controls over the computer room(s) and equipment;
3. Logical security access over infrastructure, applications, and data – operating system security and firewall management controls
4. Insurance coverage
5. Backup and recovery processes and controls also referred to as business service continuity or IT disaster recovery capability
6. System Development and System/Program change control procedure.

The purpose of this assistance is to ascertain, if the IT general control environment can be relied upon to ensure that risks of material error and/or fraud originating from the IT area and systems, are acceptable, in order for the financial auditor to rely upon computer generated financial statements.

**Table 2: Link ITGC and Financial Audit**

Government Ministries Audit File

Government Ministries (25)

Send IT Health Check Questionnaire, IT Inventory

PBA & Agencies Audit File

Public Bodies Audit & Agencies (35)

SAO – Database on Government IT Inventory/Governance Framework

Parliament Report:

Government IT Inventory Update and State of IT Governance Framework in Government Agencies

Discussion with Individual Clients

* Agree on Issue/Recommendations
* Draft Individual Report
* Update Database

**WHERE DO WE GET THE DATA TO DETERMINE AUDIT SCOPE AND STAFF CAPACITY NEEDS?**

To update and obtain information about the environment in which our auditees operate in and to guide our team’s strategic work plans, IT Inventory questionnaire are sent out to clients every two years. The purpose of this questionnaire is to update our understanding on key IT areas including key software application systems used by business cycle, existing IT Hardware, system software and IT governance framework.

For the purpose of our IT Security testing we are specifically interested in the types of operating systems and application systems used by our clients. This helps us design the most appropriate audit approach to follow and more importantly the necessary research on tools we can use to assess and audit related IT securities.

Our IT Inventory survey indicated that 4 different operating systems are used across the public sector based on responses from 50/61 government entities. Some entities use more than one operating system. The total overall responses amounted to 63.

The main operating system used by government bodies is Windows with Unix/Linux or OS400 operating systems used mainly by larger corporations within the public sector.

This same survey is used to assess team skills and competency levels in performing IT related tasks. Whist the team has basis understanding on IT Governance; it finds that it needs to continuously update its knowledge with Security controls. The rising threats to IT Systems and IT infrastructure such as computer viruses, hacking and/or unauthorized access to client systems are always present and techniques to penetrate IT systems are constantly developing. Thus, we acknowledge our technical limits as IT Auditors and respect our roles not only to enforce best practice controls and security setting but also need to grow and build our competency levels with the changes in the environment we audit.

**AUDITING SOFTWARE TOOLS:**

With limited SAI resources and based on the existing systems across the public sector, the following are the only software tools currently used by the ITA:

|  |  |
| --- | --- |
| Software Tool | Description and Purpose |
| IDEA | **Interactive Data Extraction and Analysis**This is a “general purpose” audit software tool that has a myriad of pre-programmed audit tests already built into it such as summarising, classifying, totalling, sampling, tabulating, sorting, and stratifying and so forth. As it is a general purpose CAAT tool, it can be used on any type of data from any system.  |
| MBSA | **Microsoft Baseline Security Analyser**This is a free software tool from Microsoft that enables the auditor to assess computer security weaknesses and vulnerabilities associated with the Windows Operating system. As it is a special purpose software tool, its only use is to examine Windows computer security controls |
|  DUMPSEC | Also known as DUMPACL.This is a free Windows Security Assessment software tool. It is able to read technical windows Security settings associated with users and groups and very useful if trying to see who are administrators, who has passwords, who has not changed passwords and so forth, what folders are shared between users and so forth. As it is a special purpose CAAT tool, it can only be used to assess MS Windows computer security controls |

In evaluating responses from ITGC questionnaires, we follow up on the responses and request for documentation. Additionally for all our Windows clients, we run Dumpsec to validate responses on remote access and password controls. At times, we view logs and reports within the firewalls and antivirus software used by our clients.

**SPECIFIC IT SECURITY ISSUES:**

Our clients range from small ministries employing 10 people to large corporations and ministries employee close to 1000 people. Our SAI audits about 36 public bodies and 25 government departments. Our government departments all use a centralized finance management information system administered by the Government’s Ministry of Finance. This centralized system processes, records, controls and stores all data information for the 25 government departments with additional systems used by 50% of the ministries based on their mandated roles and functions. For instance, Ministry of Revenue, Ministry of Natural Resources and Environment, the Immigration Department and so forth use other application systems. On the other hand, our government corporations use a range of systems to carry out their roles and functions.

In completing our ITGC reviews, we found IT teams within most of our clients work under the Corporate and Finance Team and primarily responsible for providing support services. The role of IT within our client environments was limited to networking with few programmers. The average number of network users across the whole public sector is about 2500 employees with 36 employees responsible for IT management supported by an additional 78 staff.

Despite the increasing significance of IT to the Samoan public sector, the inventory indicates that many agencies are not maintaining effective control over IT facilities. The general findings we noted was a general lack of overall IT strategies, lack of IT security policies, inadequate backup of information, inadequate disaster recovery plans and a lack of internet firewalls with other common findings listed in Table 3 below:

As a result of the general lack of effective control, a high risk exists in these agencies of unauthorized access to or loss of confidential data, inaccurate or incomplete data and interruption to IT operations impacting on client operations.

**Table 3: Other examples of IT Security findings:**

|  |  |
| --- | --- |
| Area | Summary of findings/audit observations: |
| IT Security Policies and Staff Awareness | Other comments provided during meetings is that the IT world in complex, our department has very few resources and its challenging having to keep up with antivirus updates especially for environments where IT infrastructure are used outside client network and a significant amount of old staff complaining about changing passwords making it difficult to enforce sound password controls and update  |
| IT Management Controls | Common findings here is that much of the work performed by IT personnel are not reported during Management meetings. The IT team reports are seen as too technical and trust is given to the IT staff to manage and respond to risks to ensure minimum disruption to work performed on IT systems and infrastructure. We found instances where:* IT staff are able to identify from system/program logs attempts by outside IP addresses to access clients email information (from Russia, Belgium) but are not included in reports to management
* Basic reports on users working after hours (after hour logs) are not provided
* Quick fixes conducted during the month/quarter are not reported in totality but summarized for management’s awareness
 |
| Network Control, Back Up Capabilities  | When reviewing/confirming (ongoing audit as of this month) user access rights into one of application systems used by one of our clients we found that the stated number of users mentioned during our interview was different from the actual user list on the system. Further enquiries revealed that they had to reinstall the application last year because of a Ramsware that caused it to fail/crash. It was during this process that old permissions were brought in but the application itself is only available on the machines of the users mentioned.  |
| IT Management Controls | The lack of system documentation and sole access by the developer to an e-voucher system used in one of our government projects impacted the ability of our client to compile financial statements when the developer passed away.  |
| Access Control | Access to EFT files for whole of government payroll payments was available to both IT and Payroll staff. Discussions with MoF about the ramifications of such security access resulted in MoF revising permissions to the file allowing only senior payroll staff to access the EFT folder |
| Network Security | The common issues using DumpSec:* Excessive administrators on the system
* Active generic user accounts
* Passwords set to never expire
* Passwords not forced to be changed
* Terminated staff still active on the system
* Logs and audit trails deactivated
* Blank userid defined to the network, etc
 |

**CHALLENGES**

**IT auditing is challenging:**

IT Audit and auditing IT Systems is not easy and requires a good understanding of IT and IS controls. Auditors not only have to be clear on the scope of the audit but need to be competent in areas discussed. They also need to be trained on how it uses, stores and reports on evidence collected during its reviews such as network diagrams, dataflow diagrams, database schemas, contract agreements, network security settings and system documentation.

**Scope creep and importance of audit planning:**

Our visits and discussions with clients IT personnel are always educational as there is always something new to document and assess (a new program, software, business need, IT infrastructure, approach and so forth). The experience and technical knowledge across our public sector varies and we quickly saw an opportunity to benchmark our weaker clients against our more matured clients.

The IT Auditors can also assist in identifying control weaknesses that create opportunities for fraud and error. These weaknesses can be a result of poorly managed and controlled IT general controls or improper application control settings applied. Based on this assessment, IT Auditors could contribute to improved efficiency and quality audits by reducing the amount of manual control testing in an attestation engagement, completing full tests of information rather than sample testing and identify appropriate sample for investigation.

However, given the various areas mentioned above and time and budget constraints there is always a challenge with execution and often times our ITA team encounters scope creep and delays in providing support work.

**Practice and Theory:**

It is not easy to apply theory and/or put ISSAI requirements into practice. There is no one size fit all although we acknowledge that there are fundamental concepts that should be embedded into any audit practice regardless of size, nature and scope.

Our review of ITGC across the public sector provides us with sufficient information about the level of ICT in Samoa and more importantly a reliable source of information to regularly assess teams’ capacity and capability levels and formulate strategy for growth and development. Just as important, IT auditors need to understand and apply fundamental auditing concepts such as materiality, documentation of assessment work performed on an IT system, root cause analysis, conclusions and ensuring complete coverage of all the relevant elements of an audit finding require improvements.

The challenges faced by our IT audit team require attention specifically with aligning/modifying ITA practice to better reflect ISSAI requirements considering the frequency of technological changes and risks to client. The onus will be on the team to communicate, strategize and propose to top management what it needs (tools, techniques, and training) in order to remain relevant and be up to date with changes in auditing IT environments.

# Road ahead from SAI Samoa

Our Office has always strived to improve public sector auditing and enhancing the quality and credibility of the work we do for our government and most importantly our people. Our ITA journeys have always been both challenging and demanding. A number of changes and projects are and/or will take place within government. The numbers of IT projects are slowing rising in respond to improved and affordable access to internet and more awareness of the values of IT. Some recent projects currently in the pipeline for some of our clients include:

1. Life Insurance and National Provident Fund are migrating from AS400 to Windows with plans to go live in May 2019 and August 2019
2. An increase in the use of electronic fund transfer payments across most of the public sector
3. Electoral voters preparing for its first electronic voting system for the next election
4. National Health Service is upgrading its Pharmaceutical Inventory system and hopes to implement a centralized system combing all the information collected by the 15 departments within NHS

This poses a question on whether or not the SAI is prepared for the upcoming changes in delivering its mandated roles and functions. Questions such as do we have the right skills and in-house capacity to audit IT systems and more importantly adequately review IT System securities, do we have the right numbers, how can we deliver our mandated roles and functions and so much more are currently been addressed.



The review of performance aspects of IT Systems and its strategic alignment to business processes goals will be necessary in the coming years. The value from IT Audits could expand to focus on business value through better understanding ICTs contribution in business processes supporting efficiency, effectiveness of ICTs within our clients. ISSAI 100 describes the role of SAI as providing assurance and comfort about the reliability and relevance of information which are used as a basis for decision making. We believe our ITA Unit will contribute to this objective by providing assurance from an IT perspective.

The role of SAI can also further developed to include advisory capacities and endorsement of better practice with ICTs to safeguard client systems and data in order to provide reliable information to enable clients to make informed decisions and generate business value. The transformation of data/ information into insights to assess needs and wants, predict behaviors and integrate it with knowledge beyond the financial statement would no doubt improve the quality of audits.

To pave the way to the future, care must be taken in developing, sustaining and retaining ITA skills and capabilities within the office. It is unfortunate that several key IT Audit staffs that were well trained during ISP are no longer with the office and only one Certified Information System Auditor exists within the office and country as a whole. To keep up with the changes in technology and to prepare the SAI for the digital age, the job descriptions for IT auditors will need to be revisited to incorporate technical knowledge and skills in IT systems and make becoming and certified IS auditor an essential requirement in becoming part of the team. These will strengthen the ability of the SAI to carry out its mandated functions and responsibilities pertaining to IT Audits.

# Why now?

Now that our Office audits and reports has been updated and our 10 year backlog has been cleared, the Controller and Auditor General (CAG) is prioritizing improvements in the quality of audits, the sustainability of institutional memory, knowledge and skills and the promotion of an organizational culture focused on consistently performing at the highest level, working harder and smarter, achieving impact and maintaining an appropriate work/ life balance.

The CAG envisions full implementation of international standards of supreme audit institutions (ISSAIs), upgrades of tools, manuals and technologies, strengthen the audit sector in the public sector through assistance to strengthening internal and external auditing across Government Ministries and Public Bodies by participating as a member of the Ministry of Finance Internal Audit Committee, peer reviews with other SAIs in PASAI and INTOSAI.

# What can WGITA do?

We strongly believe that by becoming a member of the INTOSAI Working Group on ITA will open doors for improving the work delivered by the ITA team. It will provide a valuable opportunity to train and continuous learn about the world of technology and the emerging risks associated with it. It will enhance and in many areas broaden the team’s knowledge and skills about the work of IT Auditors and most importantly it would provide a platform for encouraging assuring quality of work performed as encouraged by ISSAI 40: Quality Controls

Samoa SAI management is committed to motivating its staff to become more IT savvy and practice more data driven audit approaches. This is important because most organizations in Samoa today now work within computerized environments. The ITA team aims to increase overall SAO audit staff knowledge and competency skill levels in the areas of information technology and related controls generally.

SAI Samoa anticipates an increase in risks pertaining to client systems considering government’s reforms to strengthen, promote and encourage the use and access to the internet. This will push the economy to pursue technology enabled systems and solutions in improving its business processes. There is now an increased expectation on government auditors to provide assurance on whether such systems, processes can be trusted and have been deployed for the benefit of the country and a reasonable use of public funds.

# Conclusion

A focus on the above areas will enable SAI staff to effectively and efficiently conduct IT audit, compliance audit, project audits, performance and financial audit. This will enable our SAI to strengthen our role as government auditors and enhance the credibility and quality of our audit work. One of the key points from the Digital Pacific 2018 conference was that all representatives agreed that no one country should go through the transformation alone. The economies of scale, sharing or expertise and regional cooperation are essential for success and should be further pursued. As a SAI, we too share this notion and are now reaching out to our regional community and especially our international SAI community for assistance, guidance and continuous collaboration.

*Transformation is everybody’s job and involving all staff will accomplish the transformation*

# APPENDIX:

APPENDIX 1: SWOTs ASSESSMENT OF ITA

|  |  |
| --- | --- |
| **Strength (internal)*** There is a provision within the Audit Act 2013 to carry out Information Technology Audits
* There is a dedicated unit to conduct ITA
* Existence of operating ITA Manual, programs and work papers
* ITA currently has adequate level of understanding on what constitutes an IT Audit
* Strong understanding of Governments’ centralized accounting system
* Good data analysis skills on government accounting system which has enabled the automation of standard CAATs to be delivered for use by financial auditors
 | **Weaknesses (internal)*** The use of data by financial auditors is limited to financial audit scope
* Value of information available in data yet to be used by other operational teams
* Staff turnover both in financial audit teams and ITA teams
* Outdated ITA knowledge and skills specifically in formulating audit recommendations
* Gap between manual and actual ITA practice – improvements required considering additions/more recent changes to ISSAIs
* Lack of performance related IT Audits
* Coordination and timing of audit engagements
* **Just one Certified IS Auditor in office (former AD ITA)**
 |
| **Opportunities (external)*** Increase number of Certified IS Auditors
* Improve consistency with best practice and/or internationally recognized standards of auditing
* Improve consistency with best practice and/or internationally recognized standards of auditing
* Peer reviews to be completed by WGITA
* Support and guidance on conducting more ISSAI based ITA
* Collaborate with leading agencies in Samoa about government ICT policies, strategies and future plans
* Engage in robust discussions, interactive workshops and networking events on IT related topics
* Strengthen internal and external relationship with ITA stakeholders
 | **Threats (external)*** Increase in government legislation around ICT
* Resistance to change and fear of cyber vulnerabilities
* A dysfunction between business cycle owners and IT personnel
* Increase use of ICT in government
 |

1. <http://www.ws.undp.org/content/samoa/en/home/operations/projects/democratic_governance/together-for-a-digital-pacific0.html>

 [↑](#footnote-ref-1)
2. <http://www.ws.undp.org/content/samoa/en/home/presscenter/articles/2018/DigitalPacific.html> [↑](#footnote-ref-2)