Office of the Auditor General
CAYMAN ISLANDS

Government IT Security

September 2015

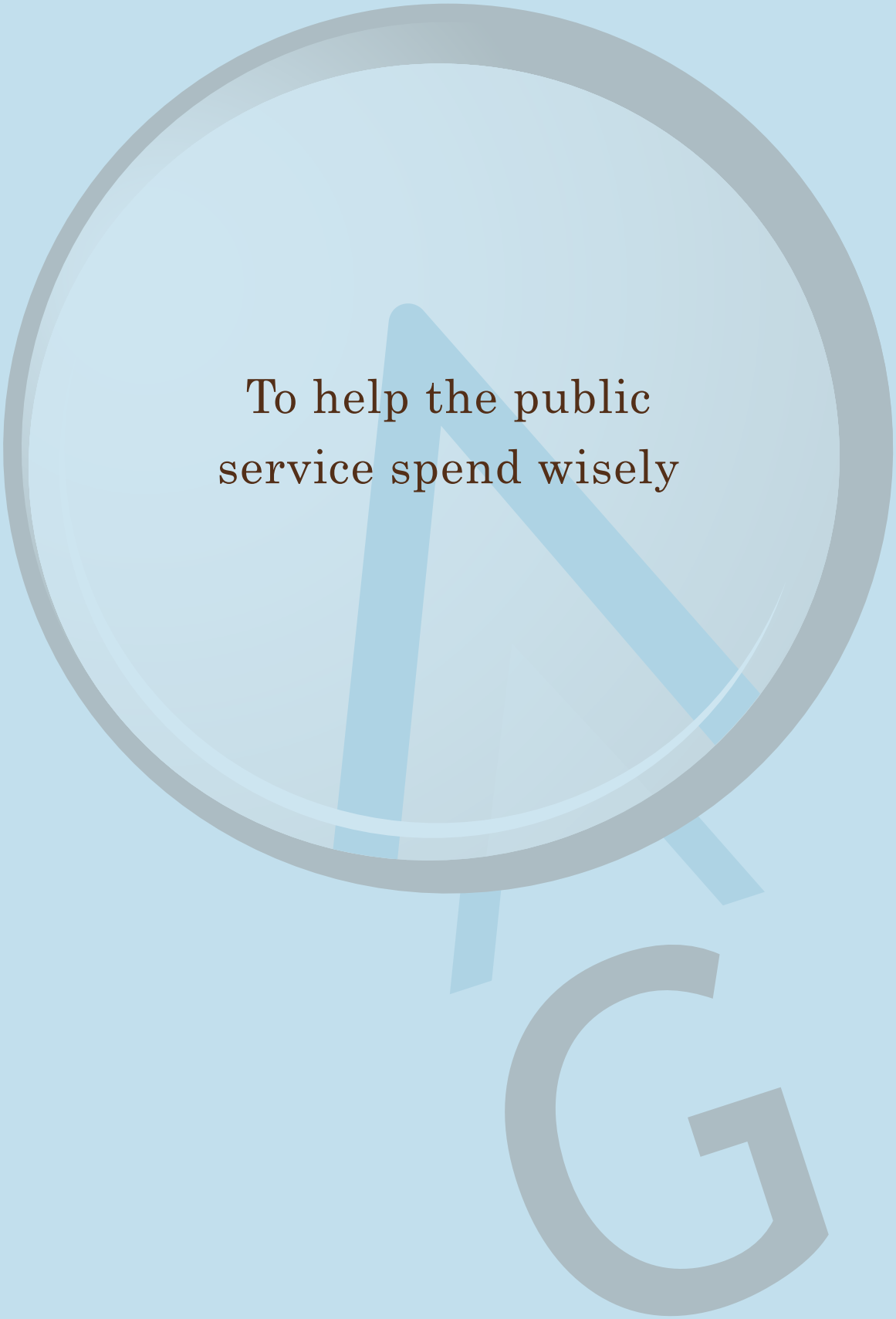

To help the public
service spend wisely

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Cayman Islands Government ("CIG") is highly dependent on information technology for the management of its business and the delivery of public services. As it looks to provide information and deliver public services more efficiently, effectively and with increased customer focus, through the use of technology and the development of its e-government programme, the demand for information technology with increased functionality and availability will continue to increase.

CIG operates a large and complex computer network that stores critical and sensitive information to enable government to function. Information is a key asset for the CIG, which needs to be managed well. This information needs to be effectively collected, processed, stored, and transmitted. Failure to protect the confidentiality, integrity and the availability of CIG's information at any stage where it is handled can result in significant reputational, operational, legal and potentially national security risks.

The objective of this work is to inform the Legislative Assembly of the vulnerability of key operational systems to security breaches and threats. We undertook an IT security assessment, following up on work we conducted in 2012 where we found significant concerns that were communicated to senior management at that time.

In 2015, we again found that the confidentiality, integrity, and availability of CIG's systems and information face significant risks and threats from attack. Whilst we noted that progress has been made in remediating some of issues identified in our original assessment in 2012, despite CIG's efforts, the overall situation requires me to report publicly on these matters.

I noted that IT governance and security has not been a priority for Government managers. Government needs to ensure that IT and information governance and security is afforded the priority it requires, and that it is seen as fundamental component in the efficient and effective management of government business and delivering public services.

Government needs to develop a clear strategy for IT and information management, establish appropriate governance structures with accountability for IT and information security, allocate the necessary resources to implement, monitor progress and periodically report to the Legislative Assembly on how well it is doing.

INTRODUCTION

1. Government's dependence on Information Technology (IT) has accelerated during the last two decades. Developments in technology have created opportunities for government to deliver greater efficiency, while keeping pace with citizens' rising expectations about how they want to engage with government and access public services and information online. In the future, we will likely see both customers and users of government IT systems demanding ever greater functionality, mobility and availability.

2. Government by its very nature is a knowledge-intensive business. Effective information technology systems are essential assets of government. Information and technology go hand in hand and are crucial to government's ability to be better informed in its decision-making, build stronger financial management and drive more cost effective delivery.

3. IT tools and techniques are used to capture, store, manipulate, communicate and use information. Government financial management and reporting relies on effective IT-based business processes to enable it to manage its finances, and enable it to make effective decisions on the allocation and use of scarce public resources.

4. Crucial to effective management of government and delivery of public service through the use of IT is: the proper protection of the operational systems and the information it stores, and providing resilience to internal and external threats. Government IT systems contain vast amounts of business critical and sensitive information, data about citizens, business and national security matters. In addition government has legal responsibilities to protect the data it manages. It is therefore fundamental that these systems are effectively protected against malicious attacks and that security is integral in their design and implementation. Failure by management to fulfill these fundamental responsibilities could lead to significant financial and reputational loss, and programmes and services not effectively delivered.

5. The importance of managing the security of Government IT systems is only going to increase as it actively looks to deliver more services online and become more customer focused, with the policy of "Digital by Default" and the ongoing development of e-government being a key government priority. Additionally the likely implementation of a data protection law will further increase the legal responsibilities of Government to manage the data it collects.

6. IT is a significant investment within the CIG. Based on the consolidated 2015-16 budget information the category of fixed assets titled computers, the cost at 30 June 2016 is estimated to be $42 million.

BACKGROUND

7. In 2012, we assessed the information technology environment and control framework for the key systems that were critical for financial management and reporting of Government. We also carried out an IT security assessment to review the vulnerability of these systems in the wider context of the CIG's IT infrastructure.

8. The findings were reported to senior Government officials in late 2012. Due to the sensitive nature of the findings we did not report the findings publicly at that time, providing Government with the opportunity to address the significant concerns we had with respect to the general IT control environment but more significantly the IT security threats Government was exposed to. At the same time, we informed officials that we would follow up this work and report publicly on the outcomes.

ABOUT THIS IT SECURITY ASSESSMENT

9. In 2015, we assessed the Government's general IT control environment, IT security and the 2013 upgrade of the Government's financial accounting system IRIS. The outcome of the work on the general IT control environment and the review of the upgrade of the IRIS system will be reported when we report on the Entire Public Sector financial statements. This report reports on the outcome of the IT security assessment.

10. The scope of the assessment on IT Security included penetration testing of the web applications, external (internet facing) network and internal (CIG internal network) network of the systems identified above.

11. We had originally planned to also include a small number of other systems relating to criminal justice and health but these were ultimately excluded for a variety of reasons, including lack of approval from external IT providers. Therefore our scope was limited as we were not able to do as wide as an assessment of IT security across Government as we had wished. However we consider our findings are still applicable to wider Government IT systems. Detailed findings from the IT security assessment were reported to senior Government officials in June 2015.

FINDINGS

WHAT WE FOUND IN 2012

12. Network security was assessed in relation to internal network security and external network (internet) security. Findings were summarized into 4 categories: high risk, medium risk, low risk and information only. See Appendix 1 for a description of each risk rating.

13. The following is a summary of the risk rating for the findings:

    - 4 high risk;
    - 15 medium risk;
    - 15 low risk; and
    - 10 informational only.

14. In summary, the observations led to an overall assessment that there were significant risks and vulnerabilities to attack to the confidentiality, integrity, and availability of the CIG's IT systems and the data that they contained. The high level risks identified can be summarized as follows:

    - external vulnerabilities to attack from individuals on the internet accessing some application data without authentication i.e. username and password;
    - internal vulnerabilities from users within the CIG network being able to access CIG databases without authentication from the internal network; and
    - an attacker being able to gain administrator level access to CIG computer servers from the internal network.

WHAT WE FOUND IN 2015

15. We found that there are still significant risks and vulnerabilities to attack the confidentiality, integrity, and availability of the CIG's systems and information that they contain. Whilst the Computer Services Department ("CSD") has made some progress in remediating the issues identified in our 2012 assessment we have found that the overall situation had deteriorated.

16. In a detailed report that we have provided to government officials, there were 33 findings with the following risk assessments:

    - 9 high risk;
    - 11 medium risk; and
    - 13 low risk.

17. The high level risks can be summarized into the following categories:

    - outdated and unsupported software in use that no longer provides the security required for government IT systems;
    - vulnerability of sensitive information from a potential cyber-attack; and
    - inappropriate configuration settings and system hardening allowing potential cyber-attackers the ability to compromise the security of the systems and services.

18. A number of the medium and lower risk observations also identified vulnerabilities that could potentially impact the confidentiality, integrity, and availability of the CIG's systems.

19. In summary the assessment indicated that management had not mitigated the significant risks and vulnerabilities around the confidentiality, integrity, and availability of the IT systems and data.

IT SECURITY ASSESSMENT

20. Whilst our assessment concentrated on the systems that could impact the integrity of financial management and reporting, the observations are indicative of significant risks facing IT systems generally.

21. The worsening situation we found is partly due to existing systems and software becoming more outdated with insufficient system and application updates creating greater susceptibility to attack.

22. We found significant need for effective leadership, strategic direction and overall management of IT across government. Our assessment found significant governance issues that need to be addressed as a top priority. For example, we found that there is no strategic plan or vision to guide the development and implementation of IT across government, to ensure it is undertaken efficiently and effectively, with security being a core component. For an entity the size of the Cayman Islands Government, this is a critical shortcoming for the management of IT resources.

23. Significant governance issues identified include:

    - Roles and responsibilities are not well defined for who has ownership of IT development across Government, and in particular for IT and information security. There is no clear accountability at a senior level and across business units for IT systems and information. The roles and relationship between CSD and business units across government are challenging. CSD does not have the capacity to effectively manage IT security, whilst managing and delivering the significant day to day business needs of government, including the development of various IT systems. The focus of government ministries, portfolios and departments are on the functionality of systems, with security being a lower priority.

- There is a lack of effective risk management practices in CSD and across government when considering IT security. No one has effectively documented and considered the IT risks across government as a whole and there is no strategy for managing the significant IT risks that the Government potentially faces. Risk management should be at the very centre of managing IT and information security.
- The development and acquisition of IT systems across Government is not guided by a strategic plan leading to ad hoc development/purchase of IT systems. CSD is usually left to reactively respond to this incremental and fragmented expansion of IT. Obviously, this impacts overall IT security and manageability.
- There is no overall investment plan that captures all of the IT purchases across Government, which ties into Government's mission in regards to IT infrastructure. Government does not know how much it costs to provide IT to all of its entities. Given IT projects are usually long-term and the cost significant, one would expect a multi-year plan to be in place.

24. A positive development in the last year has been the recruitment of a senior network security administrator; however, this critical post was vacant for over two years prior to this and much work needs to be done to address the critical issues we identified in our assessment.

25. In our assessment, we determined that IT security has not been given the high priority it needed and consequently has not been given the required resources to address the significant concerns we raised in 2012.

LOOKING FORWARD

26. Moving forward the Government needs to ensure that IT and information governance and security is afforded the priority it requires, and that it is seen as fundamental component in the efficient and effective management of government business and delivering public services.

27. At a strategic level the Government needs to consider:

    a. The development of a clear strategy for IT and information management.
    b. Establishing appropriate governance structures with accountability for IT and information security at a senior (Chief Officer) level within the civil service, and clear role and responsibilities within CSD and business units.
    c. Effective risk management practices. Risk management needs to be embedded at the centre of IT governance and the assessment IT and information security risks, directly informing effective investment in IT security. If government doesn't know what to protect, why and from whom, then it can't know if it has the proper security solutions in place. And if that is the case, it is just a matter of time before it suffers a security breach.

d. The development of risk-informed security controls which:
    i. Mitigate applicable threats.
    ii. Are kept current and actively managed.
    iii. Protect against, detect and correct malicious behaviour.
    iv. Ensure that critical technology and services are resilient to disruptive challenges such as cyber-attacks, and have the means to recover from these.
e. Development of clear IT and information security policies, including robust reporting mechanisms for data breaches and losses.
f. Raising awareness about IT and information security across the business, including the clear articulation of individual responsibilities.
g. Engaging the users with a view of making them strong links within the IT security chains, through formal security protocols that clearly outlines their responsibilities and consequences for security failures.
h. The CIG should consider adopting a security framework (e.g., a Cybersecurity Framework developed by the National Institute of Standards and Technology ("NIST") in the United States and/or Control Objectives for Information and Related Technology ("COBIT"), etc.). By adopting a security framework, the CIG will get a better understanding of the overall security posture and existing control gaps, as well as obtain a structure for the CIG's 'Defence in Depth' strategy.
i. The CIG should conduct a data/information classification exercise. The purpose of this exercise is to establish guidance for classifying CIG data based on its level of sensitivity, value and criticality to the CIG. Classification will aid in determining baseline security controls for the protection of data.

28. In terms of the specific issues identified as part of our IT assessment contained in the detailed report, CIG needs to consider the following actions:

- Develop a plan to address the observations and recommendations.
- Obtain an understanding of the reasons why these exposures were present by performing root cause analysis and implementing the appropriate procedures to ensure that these are resolved at the root cause.
- Develop and establish processes to regularly conduct risk and vulnerability assessments and review resilience planning for critical information assets, as part of a formalized vulnerability management programme.
- Take steps to implement their 'Defence in Depth' strategy including: knowing and understanding the security risks that the organisation faces; quantifying and qualifying risks; using key resources to mitigate security risks; defining each resource and its core competency; identifying and combining/adjusting any overlapping areas; adhering to existing or upcoming security standards for specific controls; and, creating and customising specific controls that are unique to the organisation.

29. Management provided a general response to our report in Appendix 2.

30. In Appendix 3, we have included management's response to the recommendations outlined below.

Recommendation #1: Prepare a strategic plan for the development and implementation of Information Technology across the Government aligned with the Government's strategic priorities, providing a clear guide for the ongoing investment and creation of value in Information Technology.

Recommendation #2: Establish an IT Governance Framework with clear accountability and responsibility for IT and information security at a senior (Chief Officer) level within the civil service. Across the entire public sector establish clear ownership and accountability for information and IT assets and expenditures as well as information security.

Recommendation #3: Develop and embed risk management practices as part of the development and management of Information Technology across the Government.

Recommendation #4: Establish annual or periodic, global assessment of the IT and data security risks faced by the Government and develop an action plan to address the key threats and vulnerabilities, including those identified in our detailed report.

Recommendation #5: Develop processes to regularly assess risk, vulnerabilities and review resilience planning for critical information assets. Monitor controls established in response to identified risks.

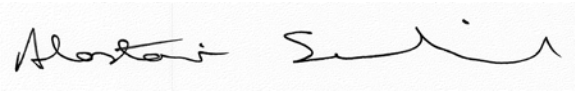
Recommendation #6: Develop and implement IT and Information security policies across Government, including robust reporting mechanisms for data breaches and losses. In conjunction with this raise awareness about IT and information security across government at all levels, and going forward ensure it is a key component of ongoing development programmes.

IN SUMMARY

31. After assessing the current risks for IT systems and data, I am concerned by the results of the findings that there is a potential for damage to government operations and its reputation. While some progress has been made in remediating the issues identified in our 2012 assessment and putting in place certain changes to improve security, the overall situation has deteriorated, and the confidentiality, integrity, and availability of CIG's systems and information still face significant risks and threats from attack both within the Government and by external sources.

32. We found that IT security has not been a priority for the Government and that is something that needs to be addressed urgently to ensure government systems and data are protected against potential threats. Moving forward, the Government needs to ensure that IT and information security is afforded the priority they require, and that it is seen as fundamental component in the efficient and effective delivery of public services. In that regard, I urge the Deputy Governor and his management team to address the recommendations in this report as a top priority.

33. The assistance and cooperation received from government officials in conducting this work is gratefully acknowledged. Without their help this work could not have been completed.



Alastair Swarbrick MA(Hons), CPFA, CFE *18 September 2015*
Auditor General
George Town, Grand Cayman
Cayman Islands

APPENDIX 1 – RISK RATINGS

The risk assessments factored in and balanced the impact of the observed vulnerability to the CIG, and the likelihood/complexity of the observed vulnerability being identified and exploited by an attacker or otherwise occurring.

The following risk rating scale is used:

High: The observed vulnerability may result in significant operational, legal, financial, or reputational impact to the CIG. The observation warrants immediate attention and the allocation of additional resources if required.

Medium: The observed vulnerability may result in operational, legal, financial, or reputational risk to the CIG. The observation warrants attention and evaluation by management. This rating includes high risk observations where the impact is mitigated by another control or where the observed vulnerability would be complex to both identify and exploit.

Low: The observation may impact on information security but is unlikely to result in operational, legal, financial, or reputational impact to the CIG. Addressing the observation will improve the CIG's security and privacy posture. This rating includes medium risk observations where the impact is mitigated by another control and where the observed vulnerability would be complex to both identify and exploit.

Informational Only: The observation is raised for management's information and to increase their understanding of the CIG's control environment. The observed vulnerability presents no appreciable risk to the CIG, or is an opportunity to improve controls.

APPENDIX 2 – COMPUTER SERVICES DEPARTMENT OFFICIAL RESPONSE

Computer Services Department (CSD) agrees with the findings of the 2015 Auditor General report on Government IT Security, and in close working with the Ministry of Home Affairs has already executed mitigation plans which has reduced or removed many of the findings from the 2015 Audit. In addition the Ministry has initiated additional IT Security reviews and commissioned an IT Governance framework centred on IT security which go well beyond the areas reviewed and commented on in the OAG audit finding and recommendations.

The OAG audit findings while limited in scope and duration (as explained in section 10) provides a clear and accurate overview of the situation at the time of the audit. CSD has only minor remarks on the findings expressed in the report (response priorities & approach). CSD would like to share that in addition to tackling the findings from the 2015 IT Audit, a tremendous effort has been expended to bolster IT security across the depth and breadth of the Government, and additional recommendations are being actioned to further entrench a culture of IT Security within CSD and across the Government.

CSD is working toward addressing these issues by:

- Researching root causes and detailing the issues and recommending solutions. We have been getting support from Ministry of Home Affairs (MHA) to address immediate issues but a multiyear plan is required and CSD is committed to delivering this,
- Through the Ministry, CSD has engaged local expertise in several areas of IT Security and Governance. The Ministry has also utilized the services of Senior Cyber Security Experts in the UK Government to assess project plans and evaluate work being done;
- Funding for training has been increased to start addressing the significant costs in IT training that are required to address the full set of problems. CSD intends to use some of this training to prepare for the implementation of the Auditor General's recommendations to the CIG executive in section 27 of the report. These recommendations include organization wide information security and risk management governance and framework compliance.
- CSD and MHA involved core customers in a retreat to start to understand the business needs of customers. CSD has also planned individual meetings with core customers to start morphing CSDs relationship with CIG business entities from service provider to business partner. This will fully align IT with government business. Over the next few months, CSD will also review the core customer's potential business strategies for the next fiscal year;
- Additionally internally developed applications and web site upgrades are being fast tracked to upgrade to supported applications. CSD staff are working on a project plan that the MHA Chief Officer, CSD Director and Deputy Director will review the plan of action and get updates on progress on a regular basis, biweekly or monthly going forward of the outstanding areas.

APPENDIX 2 – COMPUTER SERVICES DEPARTMENT OFFICIAL RESPONSE (CONTINUED)

Since moving to the MHA ministry CSD has received funding to upgrade the governments IT hardware infrastructure including some facets of security management. Additional upgrades are required on the application side. However, effective IT governance is necessary to maintain a defensive IT security posture. To this end, this CSD and MHA have been working with Deloitte to establish an IT governance within CSD and across the Government, this has spawned fourteen initiatives which are sponsored by the Chief Officer and overseen by the Project Future team.

CSD is also preparing to recruit additional IT Security related staff including a Security Project Manager. Going forward all new recruits will need to come to the table with security awareness and skills as well as increasing all CIG employees' security awareness. Since the OAG audit, CSD has expanded the network security evaluation and deployed several management tools to gain better "visibility". Our efforts have identified and addressed several weaknesses and flagged others for action by the owning agency e.g. replacing legacy hardware.

APPENDIX 3 - RECOMMENDATIONS

Recommendation	Management Response	Responsibility	Date of planned implementation
1. Prepare a strategic plan for the development and implementation of Information Technology across the Government aligned with the Government's strategic priorities, providing a clear guide for the ongoing investment and creation of value in Information Technology.	A final draft of the emergency and long term plan has been submitted to the ministry on July 17. The first version of this plan has been submitted in June. It was commented on positively by the IT Director CESG in UK. Besides addressing identified issues, the most fundamental part of the plan is the implementation of a framework. This framework will take into account most of the OAG recommendations on risk management, and root cause analysis.	Security Plan : CSD Director/ CSD Deputy Director	Implementation will be started as soon as validated by the MHA. 1st phase: Implementation of the first phase of the framework : **2 months.** This phase will determine the extent of other phases, and the schedule of next steps.

Recommendation	Management Response	Responsibility	Date of planned implementation
2. Establish an IT Governance Framework with clear accountability and responsibility for IT and information security at a senior (Chief Officer) level within the civil service. Across the entire public sector establish clear ownership and accountability for information and IT assets and expenditures as well as information security.	The necessary IT Governance response is based on 2 main axes: - Deloitte has been assigned a mission to establish a governance foundation within CSD, which fits with the Ministry of Home Affairs. Information security main objective: establish roles and responsibilities in the CSD and MHA, and promote an efficient decision making processes. - The implementation of an Information and Cyber Security Framework foundation within the whole CIG. Main objective: promote understanding of information security requirements at the highest level of the government, to insure proper alignment between mission's requirements with information confidentiality, integrity and availability and risk appetite of the various entities.	Governance : MHA Deputy Chief Officer Framework: CSD Director	1st phase : Implementation of the first phase of the Framework : **2 months.**

Recommendation	Management Response	Responsibility	Date of planned implementation
3. Develop and embed risk management practices as part of the development and management of Information Technology across the Government.	The maturity level of Risk Management in General within the CIG is at an early level. As explained in section 28 of the OAG Report, managing the risks require prior risk identification and establishment of metrics to measure them. The most fundamental step is to promote and start Information risk. Management practices is to provide awareness on the importance of Information Security Management at the highest level of the government, while informing of the de-facto accountability of the Chief Officers and Directors of proper measures to be taken to safeguard information assets. This will be achieved by the first phases of the implementation of the Security Framework, as recommended both by the CSD Security Plan and the OAG report in section 27(h.)	CSD Director	While fundamental, the required time needed to implement the foundations of a specific information risk management cannot be surely determined at this stage. It is however reasonable to estimate that initial project steps (selection of risk management framework / methodology and implementation planning) will be **started in between November 2015 and February 2016**

Recommendation	Management Response	Responsibility	Date of planned implementation
4. Establish annual or periodic, global assessment of the IT and data security risks faced by the Government and develop an action plan to address the key threats and vulnerabilities, including those identified in our detailed report.	Addressing the identified technical vulnerabilities is a must. Action plans for these identified weaknesses have been drafted and initiated, and the most critical issues have already been addressed. Addressing the root cause of the presence of these issues will be achieved by organizational measures, processes and the security framework.	CSD Director	Key threats and vulnerabilities are already all currently being addressed. Currently estimated to be completed by end of **January 2016.** Addressing the root causes: Implementation of several processes : ITIL Based Management practices, Security and Risk Management frameworks will be an **ongoing process for the next 2 years**, and the maintenance and update of these practices will require continuous maintenance in the next years

Recommendation	Management Response	Responsibility	Date of planned implementation
5. Develop processes to regularly assess risk, vulnerabilities and review resilience planning for critical information assets. Monitor controls established in response to identified risks.	A project has been assigned to a CSD member to establish ITIL based process, initially for change management, and as a later step for patch, vulnerability, and configuration management. BIA will be also introduced as a part of these processes. Periodic in-house technical Assessment has already been planned with the "Security Business Case – Phase 1", and the necessary tools have been acquired to enable efficient controls.	ITIL related Processes CSD Director (all project managers & Senior Security Administrator) Periodic Technical Security assessment CSD Director (affects entire dept.)	Periodic Technical Security Assessment plan & organization : Can be started immediately after the Firewall upgrade (**Start in September 2015**) and will require 3 months to be fully operational and documented. (**End by December 2015**) **ITIL Process and organizational structure** Initiative started, first results expected for **October 2015.**

Recommendation	Management Response	Responsibility	Date of planned implementation
6. Develop and implement IT and Information security policies across Government, including robust reporting mechanisms for data breaches and losses. In conjunction with this raise awareness about IT and information security across government at all levels, and going forward ensure it is a key component of ongoing development programmes.	As recommended both in the CSD Security Plan and in the OAG report (27.b.), assigning a CISO at the chief officer level, reporting to either the Cabinet or to the Deputy Governor is key to centralize, organize, and prioritize the various efforts initiated within the last few months within the Government. (Including Security Committee, CSD, MHA, Cabinet). The initiation of the Security framework implementation is key for the development of procedures: the policies should constitute the "law" for information assets usage and management, it is then critical to have them developed in close collaboration with the top management, to be applicable, and to obtain commitment on their enforcement.	Assigning a CISO Recommendations from CSD Director to IT Security Committee Development of Policies / Procedures MHA Deputy Chief Officer/ CSD Director	Can be started after the first milestone of Security Framework implementation (Phase 1)

Contact us

Physical Address:
3rd Floor Anderson Square
64 Shedden Road, George Town Grand Cayman

Business hours:
8:30am - 4:30pm

Mailing Address:
Office of the Auditor General
P. O. Box 2583 Grand Cayman KY1– 1103
CAYMAN ISLANDS
Email: auditorgeneral@oag.gov.ky
T: (345) 244 3211 Fax: (345) 945 7738

Complaints

To make a complaint about one of the organisations we audit or about the OAG itself, please contact Garnet Harrison at our address, telephone or fax number or alternatively email:garnet.harrison@oag.gov.ky

Freedom of Information

For freedom of information requests please contact Garnet Harrison at our address, telephone or fax number. Or alternatively email: foi.aud@gov.ky

Media enquiries

For enquiries from journalists please contact Martin Ruben at our phone number or email: Martin.Ruben@oag.gov.ky

www.auditorgeneral.gov.ky

September 2015