AUDITOR GENERAL'S DEPARTMENT
INFORMATION TECHNOLOGY AUDIT REPORT
PASSPORT, IMMIGRATION AND CITIZENSHIP AGENCY

Information Security

The Auditor General is appointed by the Governor General and is required by the Constitution, Financial Administration and Audit Act, other sundry acts and letters of engagement, to conduct audits at least once per year of the accounts, financial transactions, operations and financial statements of central government ministries and departments, local government agencies, statutory bodies and government companies.

The Department is headed by the Auditor General, Pamela Monroe Ellis, who submits her reports to the Speaker of the House of Representatives in accordance with Section 122 of the Constitution of Jamaica and Section 29 of the Financial Administration and Audit Act.

This report was prepared by the Auditor General's Department of Jamaica for presentation to the House of Representatives.

Auditor General of Jamaica
Auditor General's Department
40 Knutsford Boulevard
Kingston 5, Jamaica, W.I.
www.auditorgeneral.gov.jm

AUDITOR GENERAL'S DEPARTMENT OF JAMAICA

'A better country through effective audit scrutiny'

Document No.:	Date Submitted
AuGD354 – 1601.52.2	2021/09/16

Table of Contents

This page was intentionally left blank

Auditor General's Overview

The Passport, Immigration and Citizenship Agency (PICA) is responsible for accepting and processing passport applications, managing the island's immigration process and handling matters in relation to application for and renunciation of Jamaican citizenship. In fulfilling its mandate, the agency has adopted the use of Information Technology (IT) throughout its operations thereby creating risks that must be appropriately managed to ensure the continued availability of its services. Further, based on the nature of its operations, the agency handles personal information of its clients and national security data that should be safeguarded from inappropriate access and disclosure.

I commissioned an IT audit to determine whether PICA's information security controls were effective and will prevent or reduce the likelihood and impact of IT security risks on the organization. The audit revealed that though PICA had implemented good controls, there was room for improvement in the assessment of IT risks and access management. Additionally, PICA did not have an effective system in place for the oversight of the IT function to ensure the proper alignment of IT and corporate strategies and prioritization of its ICT projects.

This report is intended to assist PICA in improving its IT Governance and Information Security controls to effectively mitigate risks of unauthorised access and disclosure that may result in the unavailability of its systems, reputational damages and legal actions. Additionally, PICA is urged to implement the recommendations to strengthen its information security management system and ensure the confidentiality and integrity of its records.

I wish to thank the management and staff of PICA for the courtesies extended to my staff during the audit.

Pamela Monroe Ellis, FCCA, FCA
Auditor General

Executive Summary

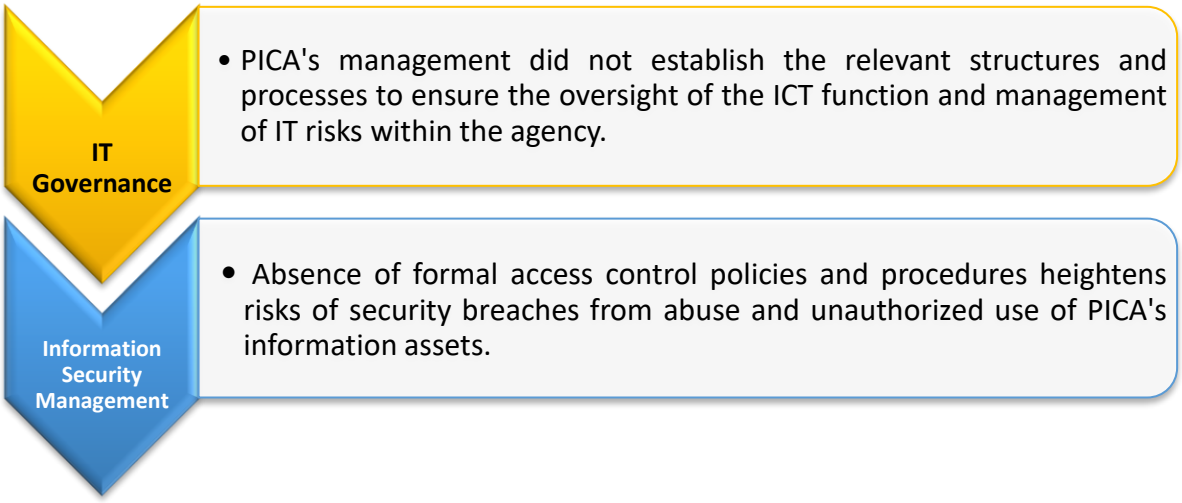
The Passport, Immigration and Citizenship Agency (PICA) accepts and processes passport applications, manages the island's immigration processes and handles matters in relation to application for and renunciation of Jamaican citizenship. Given the nature of its services and dependence on technology to enhance its efficiency, the agency must adopt a robust information security management system to ensure the confidentiality, integrity and availability of its data and systems. Additionally, the agency must establish formal governance structures to provide oversight and strategic direction in the use of technology whilst ensuring the delivery of value and management of the associated risks.

An audit of PICA was undertaken to determine whether its information security controls are effective and will prevent or reduce the likelihood and impact of IT security risks on the organization. We also assessed the effectiveness of PICA's IT governance and compliance with standards that are applicable to its Information and Communication Technology (ICT) operations.

Key Audit Question

Does PICA have effective information security controls to prevent or reduce the likelihood or impact of IT security risks?

What We Found



PICA to improve ICT Oversight and Planning

1. **PICA developed a five-year Information and Communication Technology (ICT) Road Map with proposed ICT investments of approximately US$13.3 million, but the agency did not demonstrate that a collaborative approach was taken in the review, approval and monitoring of major ICT projects.** To effectively provide oversight to the IT function, an organization should establish an IT Steering Committee or equivalent of executive, business and IT management that are responsible for prioritising IT investments, monitoring projects and service levels as well as resolving resource conflicts. PICA advised that the implementation of the projects by the ICT Unit was discussed at monthly Director's meetings, however neither the minutes of these meetings nor the progress reports were provided to assess the extent of project monitoring and strategic direction given in the execution of IT strategies.

2. Additionally, our review of the ICT Road Map revealed that ten ICT strategic goals were established, however the objectives were not clearly defined or aligned to PICA's corporate objectives for the 2018-2023 financial years. Also, whereas there was the alignment of 15 ICT projects with the corporate objectives, the relationship between the respective projects and the ICT strategic goals and objectives was not specified. Priority projects for each financial year were also not highlighted to reduce the possibility of resource conflicts and project delays. For instance, we noted in March 2021 that only four of 12 projects planned between 2018 and 2020 were completed, while the remainder were in early phases of the project management lifecycle.

> In the absence of an IT Steering Committee, PICA's oversight mechanism may be insufficient in ensuring the delivery of value from the proposed ICT investments. There is also an increased risk that ICT strategic objectives may not directly support the achievement of organizational objectives. Further, project delays and conflicts may arise from resources being allocated to activities that are not strategic priorities and or resources may not be available to execute all planned activities.

3. *Subsequent to our audit PICA established an ICT Steering Committee to improve the alignment of the Agency's ICT and business strategy and accountability for business decisions related to investments, projects, services and data.*

Unmanaged Threats and Vulnerabilities pose Information Security Risks

4. **PICA adopted an enterprise risk management (ERM) framework in its strategic planning process, which involves an analysis of technological risks to the achievement of its corporate objectives. However, formal risk assessments of its software, hardware, users, data and information were not conducted to identify and evaluate risks from ICT threats and vulnerabilities.** As a result, our audit identified instances in which the agency did not appropriately manage risks of unauthorised disclosure, abuse or misuse of access rights and environmental hazards. We found that PICA did not assess risks to its information and information processing facilities before granting employees and a third-party access to sensitive information. PICA engaged a company between 2015/2016 and 2019/2020 to deploy network

devices and perform network configurations without requiring the entity and its employees to sign a formal confidentiality or non-disclosure agreement.

5. We also noted a high dependence on the third party and Network Administrator's knowledge rather than documentation of the network topology and schematic design, which may contribute to extensive restoration delays where key personnel are separated. We also found that four new employees were given access to Government information and personal data without completing the Official Secrets Act Declaration, while standard security vetting procedures were not performed for three individuals employed for up to 3 years. Additionally, adequate environmental controls were not in place to prevent or reduce the risk of fire at two PICA locations with ICT assets valuing approximately $13.5 million. *The agency has since indicated that a confidentiality agreement will be implemented for all existing stakeholders by the end of the third quarter. PICA has also indicated that preliminary steps were taken to have the network design documented but the activity was placed on hold due to financial constraints.*

> As the agency did not apply a structured approach to its management of IT risks, we were not assured that the likelihood and impact of significant risks were appropriately evaluated, and cost-effective controls implemented as mitigating strategies. The exploitation of the vulnerabilities may result in reputational damage, loss of life, financial loss and legal actions where there is unauthorized disclosure of customers personal data.

Inadequate Security Policy Management

6. **PICA developed an ICT policy document; however, it was not extensive and bore no evidence of management review and approval.** The ICT policy document, which consist of nine topic-specific security policies, was last revised in September 2009 despite changes in technology and PICA's IT environment. We noted that the policy was not comprehensive as critical security requirements related to access control, incident response and information backup were not developed. Our audit also revealed that strict compliance with the Password Policy was not enforced as the user accounts of six ICT staff members and a director did not require periodic password changes. *Subsequent to our audit the passwords of the relevant officers were changed, however there is still no requirement within the Active Directory for periodic changes by the officers*. Given that the users have privileged access to PICA's systems, intentional or unintentional password disclosure may result in unauthorized modification of data and identity theft being undetected over a long period.

> PICA's failure to approve, periodically revise and sensitize employees of information security policies increases the likelihood that vulnerabilities may be exploited resulting in the compromise of its network and information systems.

Poor Access Control practices increases risk of Security Breaches

7. **PICA's access controls were inadequate to prevent the misuse or abuse of access rights.** International best practice recommends that a user should only be granted the rights and permissions needed to perform their tasks. However, ICT staff were assigned access rights as end users as well as administrators on the information system used to assess the validity of an applicant's photographic image, prior to the production of a passport. We further noted that user provisioning procedures were inconsistently followed as authorization requests for seven or 30 percent of the employees recruited between 2017 and 2020 could not be located by PICA. Additionally, we found that the Human Resource Department did not inform the ICT Unit of the urgent need to disable user accounts of separated staff. As a result, notifications relating to eight employees, with access to sensitive information, were sent to the ICT Unit between 29 and 386 days after the respective officer's separation date. Our analysis also revealed that the user accounts of 12 former employees were used to logon to the network for periods of up to 171 days after the relevant officer's separation. Therefore, we were not assured that an effective system was in place to prevent individuals from inappropriately receiving or maintaining access to PICA's network. *PICA has advised that Standard Operating Procedures will be revised by the second quarter, and it will include timelines for HRD to inform ICT and ICT to grant and deactivate access.*

Absence of a robust access control system may result in unauthorized access and use of confidential information. Additionally, weaknesses in the administration of user accounts combined with an insufficiently enforced password policy may result in the compromise of user accounts, unauthorized modification of records and enable identify theft.

What Should Be Done

The Passport, Immigration and Citizenship Agency (PICA) should adopt a governance framework that promotes the establishment of formal structures, to provide oversight and guide the strategic direction of the IT function to ensure the alignment of ICT and business objectives, delivery of value and risk management.

Additionally, information security management should be enhanced through the implementation and enforcement of security policies and procedures that will ensure the confidentiality, integrity and availability of its data and systems. Immediate steps should also be taken to review all user rights and permissions to ensure that access is only granted based on the roles and functions performed by employees within the agency.

Part One

Introduction

Background

1.1. The Passport, Immigration and Citizenship Agency (PICA) is an executive agency under the Ministry of National Security that plays an integral role in Jamaica's border security system. It is responsible for accepting and processing passport applications, managing the island's immigration process as well as applications for and renunciation of Jamaican citizenship. PICA is also integral to the execution of the national strategies that will contribute *to National Outcome #1: A Healthy and Stable Population* and *National Outcome #5: Greater Security and Safety* of the Vision 2030 – National Development Plan.

1.2. PICA's mission is to be an innovative, customer-oriented, strategy-focused and technology-driven organization, that through strategic partnerships will contribute to Jamaica being among the most secure countries with the best international travel experience in the Americas. The fulfilment of this mission is predicated on the achievement of the following strategic objectives over the 2018-2023 financial years:

1.3. As the agency seeks to transform its services, information technology has become a critical business-enabler as it facilitates change, encourages innovation and the adoption of new technologies. Consequently, PICA made investments in excess of $469 million in Information and Communication Technologies between April 2018 and March 31, 2020. The agency also intends to invest a proposed US$13.3 million to upgrade and implement new information systems and network equipment by March 31, 2023.

DESCRIPTION	2017/2018	2018/2019	2019/2020*
Maintenance of Computer Hardware	333,773	944,815	-
Maintenance Software & Licence	100,616,525	79,979,535	73,696,377
Computer Parts & Supplies	237,019	664,259	172,372
ICT Equipment	36,442,004	171,852,587	4,689,707
Total	137,629,321	253,441,196	78,558,456

Audit Objective, Scope and Methodology

1.4 In keeping with my constitutional mandate, an Information Technology audit of the Passport, Immigration and Citizenship Agency (PICA) was commissioned to determine whether its information security controls were effective and will prevent or reduce the likelihood and impact of IT security risks on the organization. We also assessed the adequacy of PICA's Information Technology Governance and examined, on a test basis, evidence supporting compliance with relevant policies, laws and regulations applicable to Information and Communications Technology (ICT) operations of the Agency. The review spanned the 2015/2016 to 2019/2020 financial years.

1.5 Our audit was planned and performed in accordance with the following Information Technology/Information Systems Standards for audit, governance and security:

- Information Technology Audit and Assurance Standards and Guidelines issued by the Information Systems Audit and Control Association (ISACA);
- International Standards of Supreme Audit Institutions (ISSAI) 5310: Information System Security Review Methodology issued by the International Organization of Supreme Audit Institutions (INTOSAI);
- Control Objectives for Information and related Technology (COBIT) issued by the IT Governance Institute;
- ISO/IEC 27000 family of standards dealing with Information Security Management issued by the International Organization for Standardization (ISO) and the International Electro-Technical Commission (IEC).

1.6 These standards and guidelines enabled us to test and compare the entities general computer controls against international benchmarks and widely accepted best practices within the Information and Communications Technology (ICT) sector.

1.7 Our assessment was based on the review of general IT controls, external documents, physical examinations, interviews with senior management and staff, observations and analysis of other related information.

Part Two

Information Security: Governance and Management

2.1. Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability (Figure 1)[1]. The main objective of information security is to reduce risks to an organization's information, financial, physical and human assets so that its mission can be achieved. Management therefore has a responsibility to implement the processes, policies and procedures to increase the organization's resilience, ability to respond to security breaches and ensure availability in the event of a disruption. Additionally, organizational leaders must establish structures for proper oversight and to ensure that ICT investments generate business value, risks are managed and strategic objectives are achieved.

Figure 1: The CIA Triad

Source: https://itnsconsulting.com/

2.2. The Passport, Immigration and Citizenship Agency (PICA) seeks to safeguard Jamaica's border by providing passport, immigration and citizenship services through professional, motivated staff, customer-focused processes and innovative technology. As such, the information obtained and distributed by the agency as well as the supporting IT infrastructure have become critical assets that must be protected in the delivery of its service to the nation. Further, PICA is a holder of personally identifiable information (PII) of both local and foreign travellers. As such, we expect the Agency to have a good information security governance and management system to protect its customers personal data and network from unauthorized access and disclosure. However, we found that there was room for improvement in the agency's IT governance and access controls, which are fundamental to maintaining the confidentiality, integrity and availability of its data and systems[2].

[1] NIST Special Publication 800-12 Rev.1

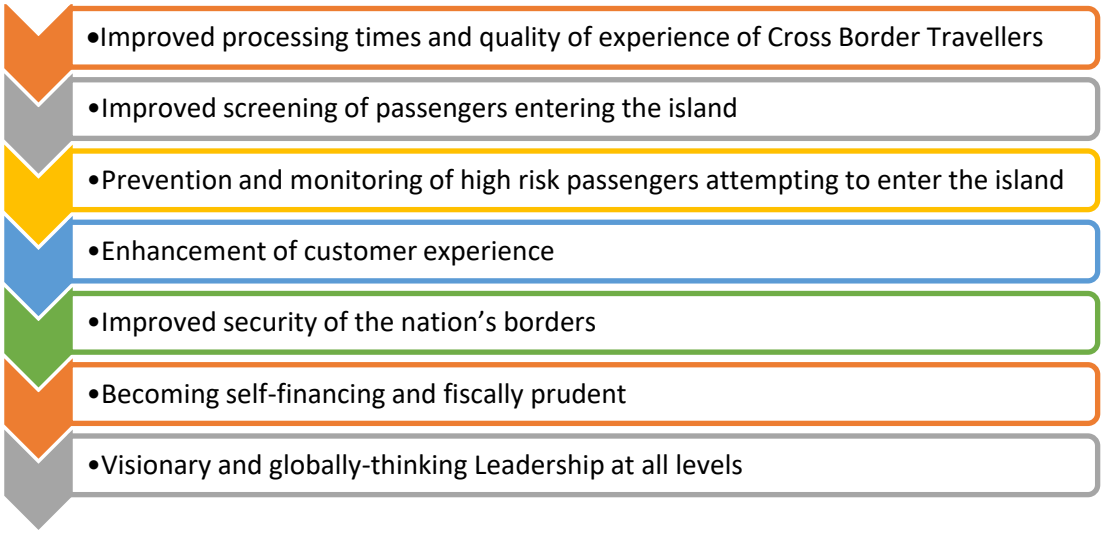
[2] Information Technology (IT) Governance is a component of Corporate Governance, which focuses on the direction and control of IT resources to ensure that organizational goals are achieved in an efficient and effective manner.

Improvements needed in ICT Oversight and Planning

2.3. Successful enterprises recognise that board and executives need to embrace IT like any other significant part of doing business. As such, there must be a collaboration between the core business and IT functions of an entity to ensure that IT investments are improving the efficiency and effectiveness of the organization, reducing risks and adding value. This requires formal oversight of the IT function to ensure the strategic alignment of business and IT objectives, clearly defined roles and responsibilities and performance measurement.

2.4. Given PICA's heavy reliance on technology to enable its business processes, we expected the agency to establish an IT steering committee (or equivalent) comprised of senior management to determine the priority of IT-enabled investment programmes in line with the entity's business strategy, track project status, resolve resource conflicts and monitor service levels and service improvements. Instead oversight of the ICT function was achieved through reviews conducted in monthly Director meetings. Our audit sought to assess the effectiveness of the practice and extent to which ICT related matters were discussed and addressed; however, neither the meeting minutes nor progress reports were provided to confirm that the performance of the IT function was sufficiently monitored. We also noted that PICA's advisory board did not include an IT professional to guide and appropriately recommend ICT strategies and risk management programs to ensure the achievement of strategic goals and outcomes.

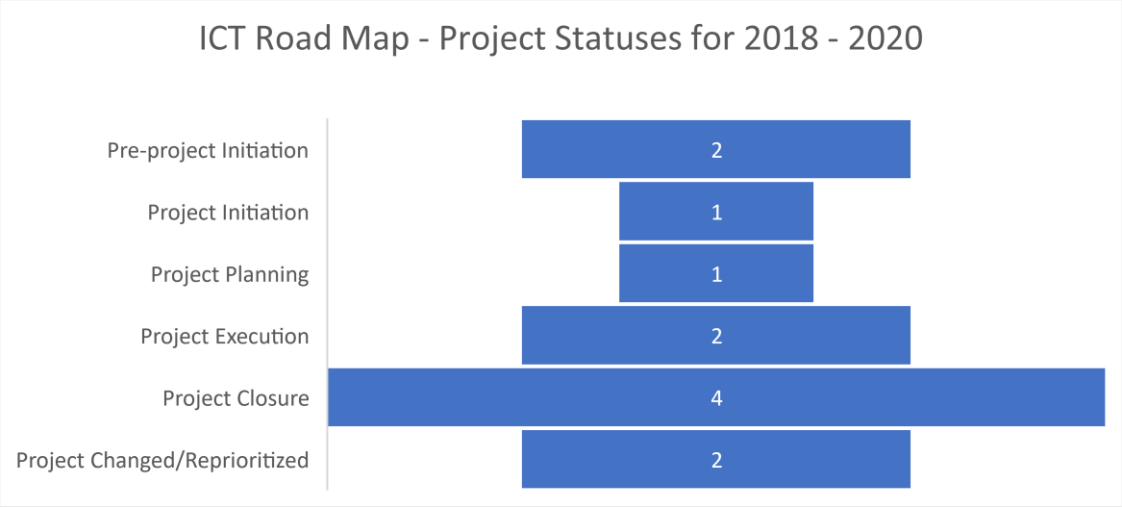
Figure 2: PICA's Strategic Outcomes 2018 - 2023



2.5. To its credit, PICA in June 2018 developed a 5-year Information and Communications Technology (ICT) Road Map *"to provide guidance on its ICT governance, enterprise architecture, enterprise systems and the targeted application of its ICT resources"*. It is envisaged that the road map will improve internal and external communication, service delivery and the ICT infrastructure. We noted that the road map outlined ten ICT strategic goals; however, the ICT strategic objectives were not clearly articulated or aligned to PICA's corporate objectives for the 2018-2023 financial periods. While we noted the relation between 15 ICT projects with estimated cost of US $13.3 million and PICA's corporate objectives, the respective projects were not linked to a specific ICT strategic objective or goal. Additionally, the road map did not identify the priority projects for each

year, which may contribute to resource conflicts and project delays. For instance, we noted in March 2021 that only four of 12 projects planned between 2018 and 2020 were completed, while the remainder were in early phases of the project management lifecycle (Figure 3). *Subsequent to our audit PICA established an ICT Steering Committee to improve the alignment of the Agency's ICT and business strategy and accountability for business decisions related to investments, projects, services and data.*

Figure 3: Summary of ICT Road Map Project Statuses

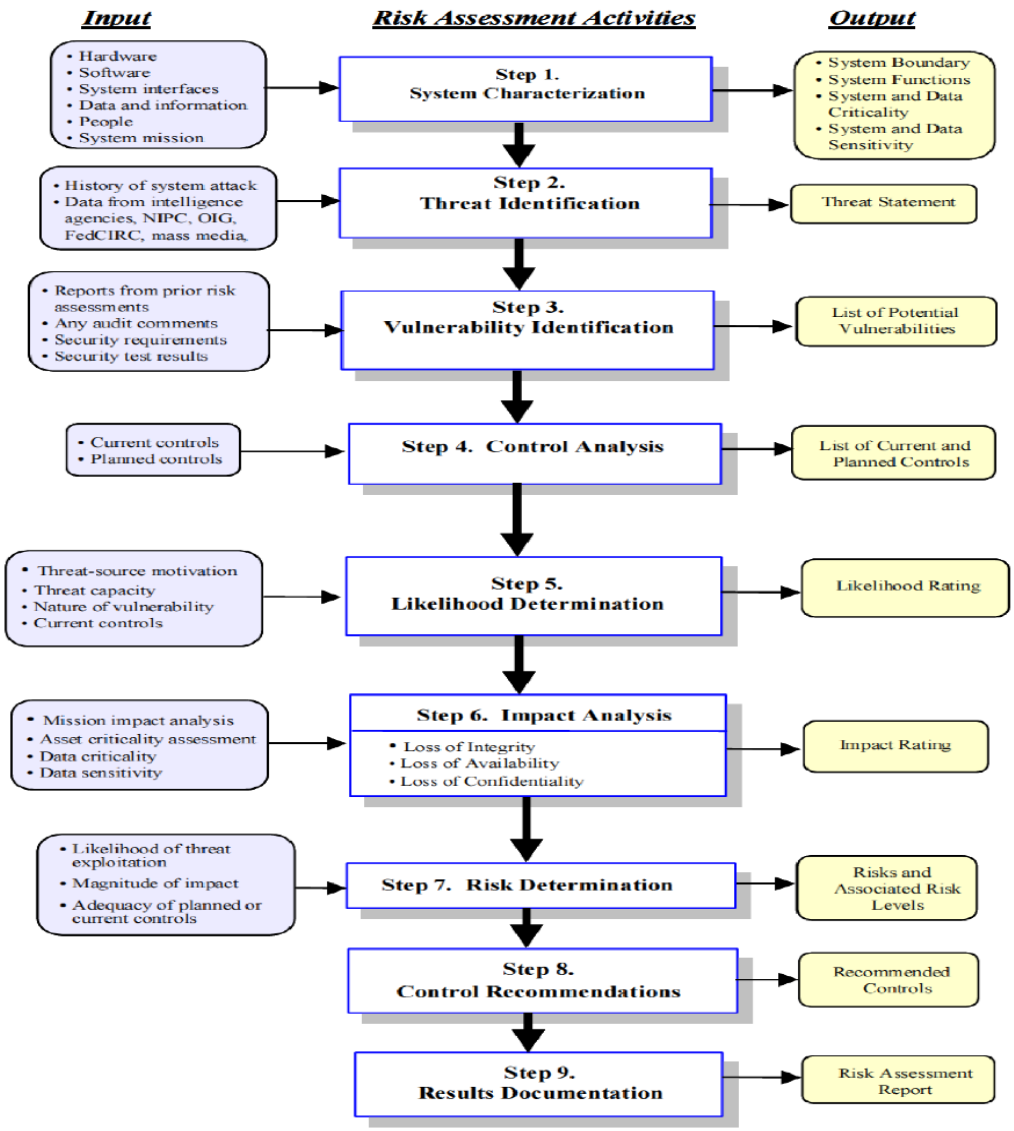


In the absence of an IT Steering Committee, PICA's oversight mechanism may be insufficient in ensuring the delivery of value from the proposed ICT investments. There is also an increased risk that ICT strategic objectives may not directly support the achievement of organizational objectives. Further, project delays and conflicts may arise from resources being allocated to activities that are not strategic priorities and or resources may not be available to execute all planned activities.

Unmanaged Threats and Vulnerabilities pose Information Security risks

2.6. Information security risks relates to the adverse impacts on an organization and its stakeholders from threats and vulnerabilities associated with the use of technology, information systems and their operating environment. An organization's leadership should therefore implement appropriate controls to manage these risks and ensure that the confidentially, integrity and availability of its data and systems are maintained. Accordingly, international best practice recommends the adoption of a systematic approach to the identification and assessment of risks, evaluation of their impact and development of mitigating strategies to reduce them to an acceptable level (Figure 4).

Figure 4: NIST Risk Assessment Methodology

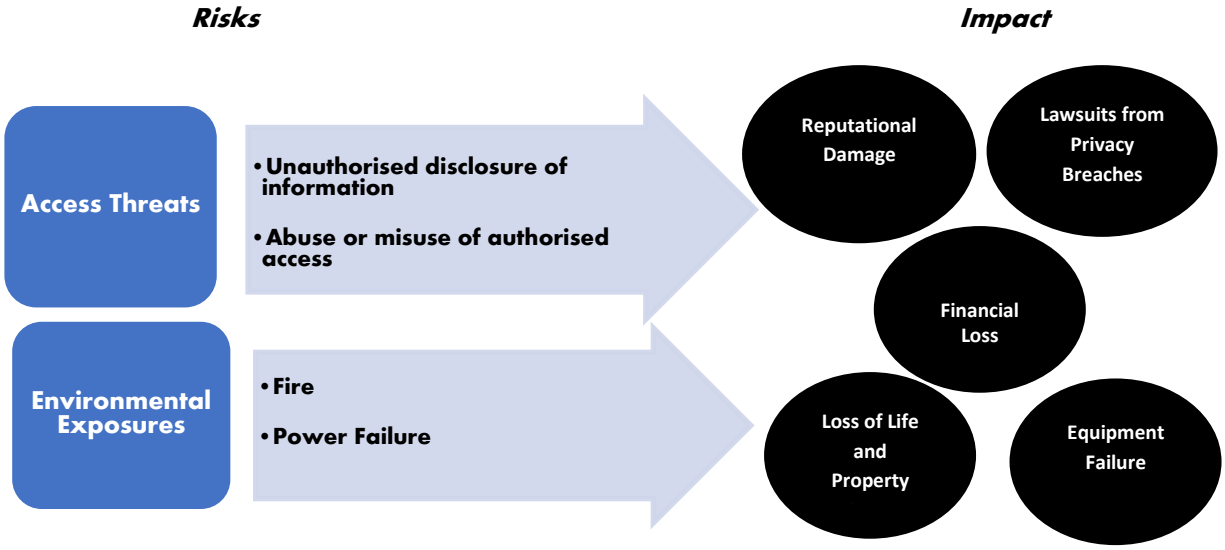


Source: National Institute of Standards Technology

2.7. As a critical agency in providing border protection and a holder of personally identifiable information, such as the name, date of birth, Tax Registration Number (TRN) and the national identification numbers of customers, we expected PICA to adopt an IT risk management framework to ensure the protection of its information assets. We noted that PICA integrated enterprise risk management in its strategic business planning process, which involved an analysis of technological risks to the achievement of its strategic objectives. However, detailed risk assessments of the entity's software, hardware, users, data and information were not conducted to determine the likelihood and impact of threats and vulnerabilities in its IT environment. Consequently, risks related to network access by third parties were not appropriately managed by the entity. We found that PICA engaged a company to deploy network devices and perform network configurations without the entity and its employees signing a formal confidentiality or

non-disclosure agreement, which would contribute to the reduction of risks from unauthorized use, access and disclosure. Additionally, we noted a high dependence on the third party and Network Administrator's knowledge rather than documentation of the network topology and schematic design. Therefore, the unavailability of key personnel may result in extensive restoration delays in the event of a major network disruption, especially considering the lack of a formal backup strategy. *Since our audit, PICA has taken preliminary steps to have the network design documented but the activity was placed on hold due to financial constraints.*

Figure 5: Impact of PICA's Unmanaged Risks



2.8. We also found that the confidentially of PICA's information was threatened with four employees being granted access to personal data and government information without completing an Official Secrets Act Declaration, which is intended to restrict the unauthorised disclosure of information obtained while employed to a public sector organization. Our review also revealed that PICA's security vetting procedures were not performed for three candidates who were employed to the agency for up to 3 years[3]. *The agency has since indicated that a confidentiality agreement will be implemented for all existing stakeholders by the end of the third quarter.*

2.9. In the absence of an IT risk assessment, our audit also revealed that PICA did not implement the relevant controls to reduce environmental risks to its assets at two of its locations. Inspection of one location, including server room and wiring closets, revealed that no fire suppression equipment was installed to mitigate the risks to PICA's human and technological assets. The agency also did not provide evidence that two Uninterruptible Power Supply (UPS) costing approximately $3.5 million were subject to periodic maintenance to ensure optimal performance in the event of power surges or failures. Additionally, we found that the fire extinguishers at another location were last serviced in 2016 and 2017, which may result in the equipment not operating during an emergency. If these environmental risks were to materialize, PICA could lose approximately $13.5

[3] PICA's standard operating procedures for recruitment and selection requires a criminal record from the Jamaica Constabulary Force. If satisfactory, the Revenue Protection Division (RPD) or its internal Investigation and Surveillance Unit (ISU) further vets the individual's background prior to preparing an offer letter or contract.

million, which was invested in ICT assets for the relevant locations over the last three years. *Subsequent to our audit the agency serviced and acquired fire extinguishers for the relevant locations, however PICA does not have a formal agreement in place for periodic inspection and maintenance of the equipment.*

As the agency did not apply a structured approach to its management of IT risks, we were not assured that the likelihood and impact of significant risks were appropriately evaluated and cost-effective controls implemented as mitigating strategies. The exploitation of the vulnerabilities may result in reputational damage, loss of life, financial loss and legal actions, where there is unauthorized disclosure of customers personal data.

Inadequate Security Policy Management

2.10. A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties[4]. Information security policies represents managements intention to direct and control the operations of the organization in order to preserve the confidentiality, integrity and availability of its data and information systems. Additionally, policies should consider requirements created by the organization's business strategy, legislation and regulations, contractual obligations as well as the current and projected information security environment.

2.11. PICA's IT function developed an ICT policy document, comprised of nine topic-specific policies, however the agency could not provide any evidence of management's review and approval. Additionally, despite the organization's adoption of new technologies and changes in the ICT environment over the last decade, the policies were last revised in September 2009. We also noted that though the policies were made available to staff, PICA did not conduct periodic sensitization sessions to improve security awareness, culture and compliance of all users. The ICT policy was also not comprehensive as information security requirements related to access control, incident response and information backup were not addressed. Of note, we found that all ICT members and a director had their passwords set to never expire for up to six years and four months, in contravention of the agency's password policy (Table 1).

Table 1: FRS Users with Non-Expiring Passwords

USER	PERIOD ELAPSED SINCE LAST PASSWORD CHANGE
Senior ICT Officer 1	6 yrs. 4 mths.
Junior ICT Officer 1	4 yrs. 11mths
Senior ICT Officer 2	3 yrs. 2mths
Director 1	2 yrs. 9 mths
Junior ICT Officer 2	1 yr.10 mths.
Senior ICT Officer 3	9 mths.
Junior ICT Officer 3	5 mths.
Junior ICT Officer 4	1 mth.

[4] ISO/IEC 27002 Information Technology Security Techniques - Code of practice for information security controls

2.12. *Subsequent to our audit the passwords of the relevant officers were changed, however there is still no requirement within the Active Directory for periodic changes by the officers*. In the context where these users have privileged access to PICA's systems, intentional or unintentional password disclosure may result in unauthorized modification of data and identity theft being undetected over an extended period.

PICA's failure to approve, periodically revise and sensitize employees of information security policies increases the likelihood that related vulnerabilities may be exploited resulting in the compromise of its network and information systems.

Poor Access Control practices increases risk of security breaches

2.13. Good information security management is dependent on an effective risk management process as the implementation of relevant controls will reduce the impact of threats and vulnerabilities within the organization's environment. Employees represent the greatest security vulnerability as, data and information may be intentionally or unintentionally shared and authorised access may be misused or abused. Consequently, a formal access control policy should be established and based on the principles of least privilege or "need-to-know" and "need-to-use". However, our audit identified weaknesses within PICA's access control practices that may threaten the confidentiality, integrity and availability of the agency's data and systems.

2.14. Given that PICA holds confidential information for its customers and employees, we expected the agency to implement strong controls to ensure that its information assets were appropriately safeguarded. At a minimum, access should be authorized based on the role and functions performed by an employee. However, ICT staff were assigned access rights that were inconsistent with the principle of least privilege, which dictates that a user should only be granted the rights and permissions needed to perform their tasks. We found that ICT staff were added as members of the operational user group as well as the administrator group for an application, which is used to assess the validity of the photographic identity of an applicant, prior to the production of a passport. The lack of a formal access control policy and the deviations from the password policy identified may result in the compromise of user accounts and unauthorized changes.

2.15. Additionally, international best practice recommends the implementation of a formal user access provisioning process to assign or revoke user access rights for all user types to all systems and services[5]. Accordingly, it requires the maintenance of a central record for access rights granted to a user as well as the restriction of access, prior to completion of authorization procedures. User accounts should also be immediately disabled once a user has left the organization. However, from a sample of 21 new employees, PICA was unable to locate authorization requests for seven or 30 percent of the employees recruited in management positions between 2017 and 2020. Similarly, the separation notifications for eight of 27 former employees were not presented during our audit (Table 2).

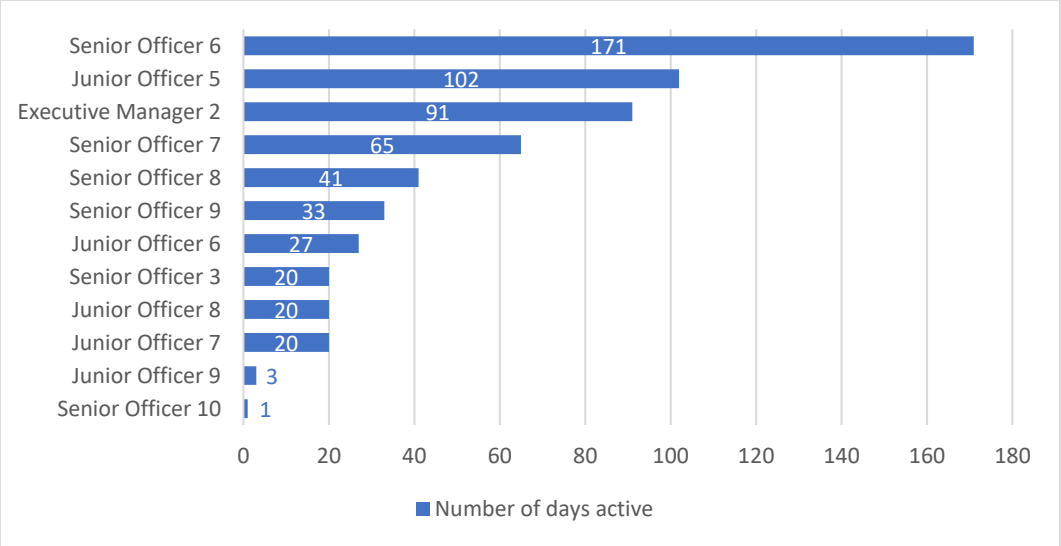
[5] Section 9.2.2 of ISO/IEC 27002 Information Technology Security Techniques – Code of practice for information security controls

Table 2: New and Separated Employees without Access Notifications

User	Date	Employment Status
Senior Officer 1	October 2, 2017	New
Executive Manager 1	January 2, 2018	
Senior Officer 2	April 1, 2019	
Director 2	April 2, 2019	
Director 3	July 1, 2019	
Senior Officer 1	January 6, 2020	
Senior Officer 2	January 6, 2020	
Temporary Officer 1	July 1, 2019	Separated
Junior Officer 1	August 2, 2019	
Junior Officer 2	August 27, 2019	
Junior Officer 3	September 10, 2019	
Junior Officer 4	October 1, 2019	
Senior Officer 3	August 22, 2019	
Senior Officer 4	September 23, 2019	
Senior Officer 5	October 9, 2019	

2.16. Also, the Human Resource Department (HRD) was consistently tardy in advising the ICT Unit of separations as notifications relating to eight other employees were sent between 29 and 386 days after the respective officer's separation date. Further analysis also revealed that the user accounts of 12 former employees, with access to sensitive information, was used to logon to the network for periods of up to 171 days after the relevant officer's separation. Consequently, we were not assured that an effective account administration system was in place to prevent individuals from inappropriately receiving or maintaining access to PICA's network. *PICA has since advised that the Standard Operating Procedures will be revised by the second quarter, and it will include timelines for HRD to inform ICT and ICT to grant and deactivate access.*

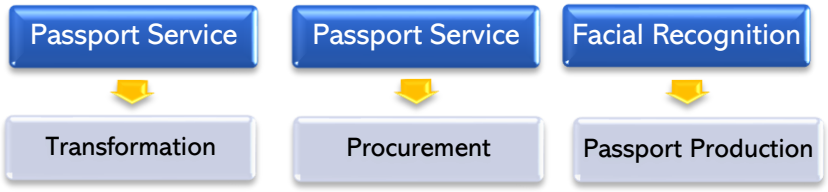
Figure 4 : Users with Active Network Accounts after Separation



2.17. We also found that the accounts of separated immigration staff were not disabled on an application used to record sensitive information such as, passenger entry and exit, work permits and watch list for persons of interest. Contrary to best practice on segregation of duties, we found

that process owners performed system administrator duties instead of a member of the ICT Unit. As a result, the addition and removal of application users was performed by the respective unit heads. Our review also revealed that 17 individuals previously employed in the Immigration Services Unit had a total of 67 user accounts of which 35 or 52 percent were active at the time of our audit (Appendix 1). Additionally, we found that poor user management practices resulted in three senior officers retaining access to the Facial Recognition System (FRS) though they were reassigned to other departments and access was no longer in line with their job function. Of note, similar weaknesses were identified by the Agency's Internal Audit Unit in August 2017, however the account administration process was not regularized at the time of our review.

Figure 5: Reassignment of staff with access to the Facial Recognition System (FRS)



Absence of a robust access control system may result in unauthorized access and use of confidential information. Additionally, weaknesses in the administration of user accounts combined with an insufficiently enforced password policy may result in the compromise of user accounts, unauthorized modification of records and enable identify theft.

Appendix 1: Separated staff with active network and application user account

No.	Post	*Separation Date*	Number of Active Application Accounts
1.	Senior Officer 6	03 Sep 2018	1
2.	Junior Officer 5	27 Aug 2019	1
3.	Executive Manager 2	30 Apr 2018	5
4.	Senior Officer 7	23 Sep 2019	2
5.	Junior Officer 6	01 Apr 2019	2
6.	Senior Officer 11	01 Jan 2018	1
7.	Junior Officer 10	01 May 2018	1
8.	Senior Officer 12	23 Aug 2018	4
9.	Junior Officer 1	02 Aug 2019	1
10.	Junior Officer 4	01 Oct 2019	2
11.	Senior Officer 13	12-Oct-17	3
12.	Senior Officer 14	25-Jan-18	3
13.	Junior Officer 11	25-Sep-19	4
14.	Junior Officer 12	23-Nov-18	1
15.	Junior Officer 13	17-Aug-18	2
16.	Junior Officer 14	29-Jul-19	1
17.	Junior Officer 15	2-Jan-20	1
			35

Source: AuGD Analysis

This page was intentionally left blank