N A O
National Audit Office
MALTA

Information Technology Audit

Cyber Security across Government Entities

Report by the Auditor General

February 2017

N A O
National Audit Office
MALTA

Information Technology Audit

Cyber Security across Government Entities

Table of Contents

Annexes

List of Figures

List of Tables

LIST OF ABBREVIATIONS

The following is a list of abbreviations, which are used inter-alia throughout the document.

BCP	Business Continuity Plan
BYOD	Bring-your-own-Device
CCTV	Closed Circuit Television
CDRT	Centre for Development, Research and Training
CIMU	Central Information Management Unit
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
CRPD	Commission for the Rights of Persons with Disability
DRP	Disaster Recovery Plan
e-mail	Electronic Mail
eRFS	Electronic Request for Service
EU	European Union
HR	Human Resources
ICT	Information and Communications Technology
IMU	Information Management Unit
IP	Internet Protocol
IPS	Institute for Public Services
IT	Information Technology
LAN	Local Area Network
MAGNET	Malta Government Network
MCAST	Malta College of Arts, Science and Technology
MCCAA	Malta Competition and Consumer Affairs Authority
MITA	Malta Information Technology Agency
MQF	Malta Qualifications Framework
NAO	National Audit Office
NAS	Network Attached Storage
OS	Operating System

PAHRO	Public Administration Human Resources Office
PC	Personal Computer
PRTG	Paessler Router Traffic Grapher
REWS	Regulator for Energy and Water Services
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network

Executive Summary

Executive Summary

Over the past five years the National Audit Office has conducted a number of IT audits in various Government departments and entities. Certain findings were common across the different IT audits, in particular, the lack of Cyber Security Controls or, in other words, the lack of controls protecting Government departments and entities' exposure to both external vulnerabilities and intrusions as well as internal breaches and disclosures. The extent to which entities were adequately positioned to address such threats was often a cause of concern.

Within this context, the NAO embarked on a horizontal audit to compare the level of adoption of selected Cyber Security controls across selected auditee sites. The horizontal audit was conducted across the following 10 different Government entities:

- Malita Investments p.l.c.
- Malta College of Arts, Science and Technology.
- Malta Competition and Consumer Affairs Authority.
- Malta Enterprise Corporation.
- Malta Freeport Corporation Ltd.
- Manoel Theatre.
- Commission for the Rights of Persons with Disability.
- Refugee Commission.
- Regulator for Energy and Water Services.
- WasteServ Malta Ltd.

Key Findings

Chapter 1 provides information about the Government entities reviewed with respect to their business processes, the type of data being processed by each entity and their respective IT infrastructure. The NAO noted that small Government entities are opting to fully out-source their IT services and practically have no in-house IT resources to manage these out-sourced services and the entity's IT requirements and related risks. The NAO further observed that some entities do not even have basic information regarding their IT set up, such as a local area network diagram. It is also evident that there is an increasing popularity of cloud computing with four entities opting for a cloud-based e-mail service. Furthermore, one of these entities also opted to use different cloud-based services to host its main software application, its accounting data and the data owned by its Administration Department. Whilst the NAO understands the flexibility, accessibility and storage potential that these services offer, it would like to highlight the importance of '*reading the small print*' in the binding agreements signed with respective suppliers, and the need to clarify the hosting country of one's data. (Personal or sensitive data being hosted outside Europe would need to be declared to the Data Protection Commissioner). The NAO noted MITA's intention[1] of exploiting cloud-based approaches and implementing a Cloud strategy for Government, and recommends that the latter is issued as soon as possible.

Chapter 2 evaluates the controls adopted to maintain confidentiality, integrity and availability of data, and delves into data retention policies. The NAO observed that only one of the 10 audited entities had a Data Retention and Storage Policy and in this instance, the policy was under review and not being adopted. Similarly, the NAO noted that only one entity had an Information Classification Policy. The lack of such policies is resulting in entities not appreciating the importance and criticality of their data and thus, are unaware of the need to implement controls that maintain confidentiality, integrity and availability, based on the criticality of that data. This situation could potentially lead to non-compliance with the Data Protection Act. The NAO is also concerned with the lack of adequate hardware disposal procedures, with hard-disks being sometimes discarded prior to being rendered unreadable.

Chapter 3 reviews initiatives related to Cyber Security awareness, looking into training, user manuals and policies available to users at the auditee sites. The NAO observed a general lack of user awareness initiatives. Given that 60%[2] of all Cyber Security attacks are known to be stemming from 'insiders', the NAO recommends that user awareness is afforded greater importance. Furthermore, the NAO noted that three entities do not have any Internet and e-mail usage policies. These policies regulate the personal use of Government e-mail and ensure accountability on the use of Government Internet services.

Chapter 4 reviews malware and anti-virus protection, as well as patch management and controls related to portable media devices. The NAO noted that most of the audited entities do not appreciate the importance of patch management and some were under the false belief that their anti-virus software protects them against all threats. Furthermore, the NAO observed that most entities are not regulating the use of portable storage media devices and limiting or discouraging the connection of such devices to the entity's network except where there is a valid business case for their use.

Chapter 5 looks into business continuity plans in place at the auditee sites. The NAO noted that none of the audited entities had a Business Continuity and Disaster Recovery Plan[3]. Furthermore, the NAO was disappointed to note the lack of importance given to the recovery of data, with only five of the audited entities performing some type of data restore testing from backup (although in most cases not all backups were restored). Moreover, the NAO noted that only four of the audited entities are storing their backups offsite, with the majority keeping their backup media in proximity of their servers.

[1] https://mita.gov.mt/en/Documents/MITA%20STRATEGY%202015-2017.pdf

[2] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF

[3] One entity had a documented set of procedures outlining the importance of such plans.

Chapter 6 covers IT hardware and software inventory management, physical security and server monitoring. The NAO observed a general lack of adequate IT hardware and software inventories, with 50% of the entities audited not having a software inventory. The NAO also noted the lack of adequate server rooms, observing that one particular entity had a server room that was next to an internal courtyard, with no adequate apertures and thus prone to flooding or pest infestation. Other server rooms were cluttered or used as hardware or document repositories. Furthermore, the NAO observed that three of the audited entities did not have a server room on their premises and their servers were situated in offices. The NAO noted a general lack of server and network monitoring which was being carried out only in four of the audited entities. In most of the cases this lack of monitoring stems from lack of IT resources. Network and server monitoring is one of the most essential tools in protecting an entity against Cyber Security threats, as through such monitoring one can identify any unauthorised access attempts, file modification attempts and any kind of denial of service attacks.

Chapter 7 reviews the level of access control management (i.e. management of logins and passwords for the IT systems used at the auditee site). The NAO noted that in most of these sites, the GMICT Password Policy[4] issued by MITA is not being followed in terms of password complexity, password expiry, password history and the need to force the user to change his/her password upon first logon. Two entities did not implement any password complexity rules, neither on their PCs nor on their software, whilst another four entities opted to implement password complexity rules when logging onto their PC's and when accessing e-mails, but not in order to access their software applications. Furthermore, the majority of the entities audited are not following the standard naming convention in terms of usernames.

Finally, **Chapter 8** lists all the Management Comments submitted by the 10 audited entities and includes an Implementation Strategy indicating the dates by which the recommendations detailed in each Chapter are to be implemented. The NAO was pleased to note that most of the feedback given to the auditees was taken on board and some of the entities even embarked on improving their situation while the audit was still underway.

As indicated throughout the report, the Government entities that are considered to be the most prepared against Cyber Security threats are:

- Malta Enterprise Corporation.
- WasteServ Malta Ltd.
- Regulator for Energy and Water Services.
- Malta College of Arts, Science and Technology.

On the other hand, the NAO recommends that the other entities which have participated in this audit review their IT operations as soon as possible with the aim of improving their level of preparedness toward Cyber Security, thus, ensuring that this audit's principal objectives would be attained.

[4] https://mita.gov.mt/en/GMICT/Pages/Security.aspx

Given that the results stemming from this horizontal audit are similar to the ones emanating from the full IT audits that the NAO has concluded in the past, especially those conducted in Government entities, the NAO is considering these audit findings as highly indicative of the scenario and has thus rated each criteria examined in this audit, for each of the 10 audited sites, using a Maturity Model so as to provide a general picture indicating where Government entities are positioned in terms of Cyber Security (Figure 1).

The NAO strongly recommends that each Ministry CIO, in collaboration with the respective entity's Head, embarks on an exercise to address the major weaknesses identified and reported upon during this audit. Furthermore, the NAO suggests that MITA should consider the type of support it could provide CIOs in addressing the weaknesses in the following areas:

- Business Continuity and Disaster Recovery.
- Data Retention and Data Storage.
- Information Classification.
- User awareness and User Manuals.
- IT Hardware and Software.
- Portable storage devices.
- Adequacy of Server Room.
- Recovery of Data.
- Entity's IT Resources.
- LAN.
- Internet and e-mail usage.
- Server and Network Monitoring.
- Hardware Disposal.
- Unauthorised physical access.
- Storage of Backup media.

The recommendations detailed in this report are based on findings from fieldwork at the selected Government entities, and are likely to be relevant to other Government entities including Government ministries and departments. Therefore, Ministry CIOs are encouraged to assess the benefits of implementing these recommendations in light of their own particular circumstances and business. risks.

[5] Key to Figure 1 (below)
Each criteria was rated for every entity using a grading scheme whereby:

- 0 – Controls not in place
- 1 – Controls partially in place
- 2 – Controls partially implemented
- 3 – Controls fully implemented
- 4 – Controls reviewed and improved periodically as part of the entity's normal business process.

The resulting figures plotted below are the summation of these ratings, across all entities for each audited criteria.

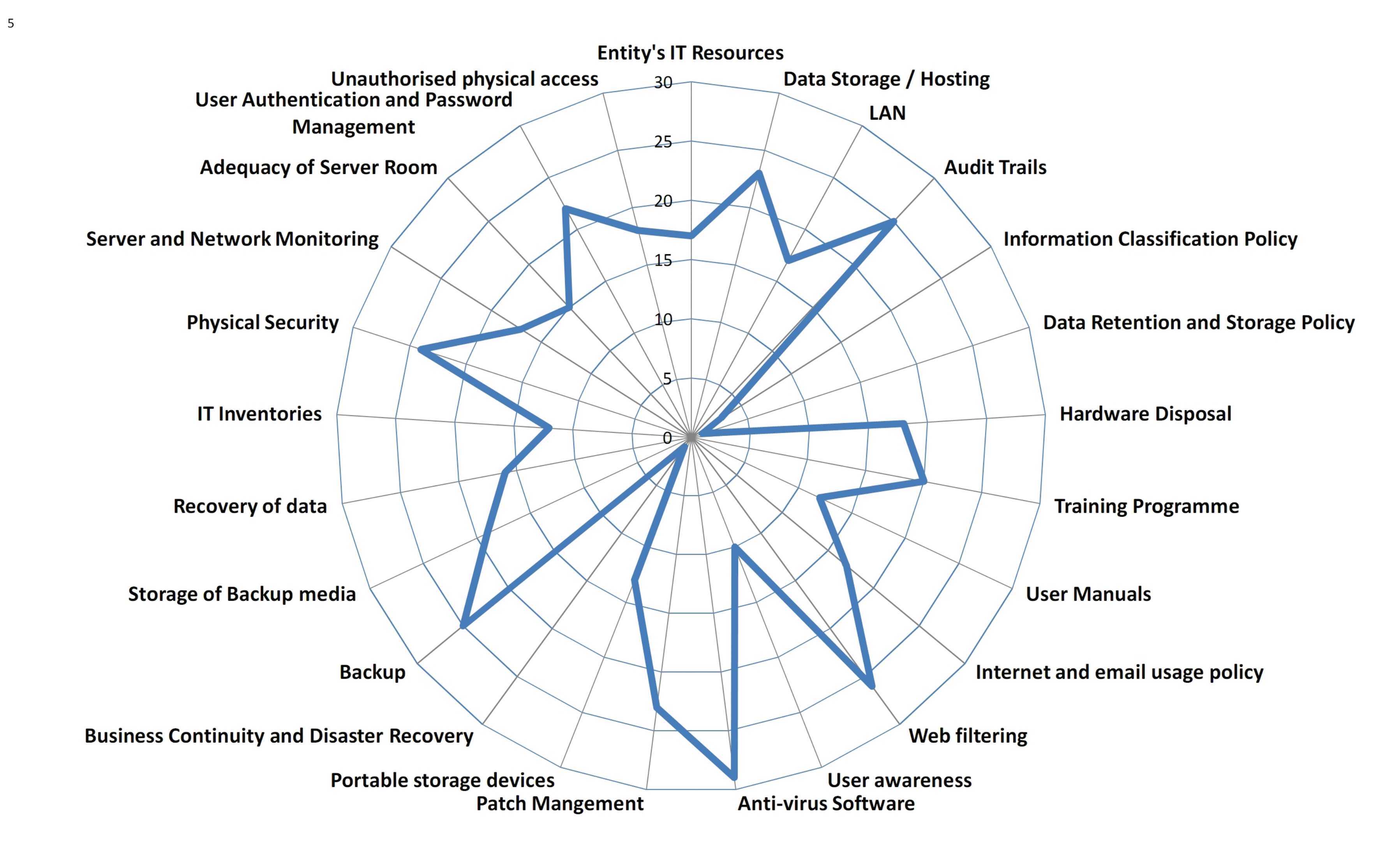


Figure 1: Cyber Security across Government entities

Chapter 1

Overview

Chapter 1

Overview

This Chapter provides background information about the audit. It also lists the Government Entities reviewed as part of this horizontal audit and details their business process, the type of data being processed by each Entity and the IT infrastructure within each Entity.

Furthermore, this Chapter includes the Audit scope and objectives and describes the methodology used in attaining the audit objectives.

1.1 Background

The National Audit Office (NAO) has conducted a number of IT audits in various Government Departments and Entities. During these audits the NAO noted that there seemed to be a trend of findings in certain areas. It also noted that Government Entities (excluding Government Departments) tend to have findings of a more critical nature in terms of Cyber Security.

It was thus decided that, a horizontal audit, across 10 different Government Entities, with the portfolio of different Ministries, is carried out so as to obtain a better understanding of the level of Cyber Security amongst Government Entities.

This audit document is structured in such a way that highlights the recommendations that may apply to all Government Entities. The NAO suggests that the Ministry's Chief Information Officers (CIO) encourage the implementation of such recommendations and set a basic level of Cyber Security across all the Entities under their portfolio.

1.2 Audit Coverage

The Entities, including respective Ministries under which they fall, covered during this audit were:

- Malita Investments p.l.c. – Ministry for Finance.
- Malta College of Arts, Science and Technology (MCAST) – Ministry for Education and Employment.
- Malta Competition and Consumer Affairs Authority (MCCAA) – Ministry for Social Dialogue, Consumer Affairs and Civil Liberties.
- Malta Enterprise Corporation – Ministry for the Economy, Investment and Small Business.
- Malta Freeport Corporation Ltd. – Ministry for Competitiveness and Digital, Maritime Services Economy.
- Manoel Theatre – Ministry for Justice, Culture and Local Government.
- Commission for the Rights of Persons with Disability (CRPD) – Ministry for the Family and Social Solidarity.
- Refugee Commission – Ministry for Home Affairs and National Security.
- Regulator for Energy and Water Services (REWS) – Office of the Prime Minister – Energy and Projects.
- WasteServ Malta Ltd. – Ministry for Sustainable Development, the Environment and Climate Change.

1.2.1 Malita Investments p.l.c.

Malita Investments p.l.c. was incorporated in June 2011 as a Maltese public limited liability company to operate on an independent and commercial basis, in an initiative aimed at long-term investment development in Malta and the private sector, with the principal purpose, inter-alia, of acquiring, developing, managing and operating immovable property.

In 2011, Malita Investments p.l.c. was capitalised by the Government of Malta through a €25 million cash injection. In June 2012, the Company and Government entered into two transfer contracts pursuant to which it acquired from Government the title of dominium directum over the Sites of the Valletta Cruise Port and Malta International Airport, and the Company issued in favour of Government an aggregate amount of 68,108,064 fully paid up Ordinary A Shares of a nominal value of €0.50 per share.

On 26th June 2012, the Company entered into a public deed with Government pursuant to which the Company acquired the 65-year utile dominium over the Parliament Building and the Open-Air Theatre. On the same day, the Company as lessor and Government as lessee, entered into the Lease Agreements where Government agreed to lease out the Parliament Building for an automatically renewable period of 20 years and the Open-Air Theatre for an automatically renewable period of 30 years.

In July 2012, the Company made an issue of 30,000,000 Ordinary B Shares of a nominal value of €0.50 per share to the public, which were fully subscribed.

In the meantime, the Board of Directors continued to consider and evaluate a number of potential projects including ones with a mix of public/private participation.

1.2.2 Malta College of Arts, Science and Technology

Established in 2001, the MCAST is the country's leading vocational education and training institution. Through its three Colleges, namely the Foundation, Technical and University Colleges, and the six Institutes in Malta and the Gozo Campus, it offers 180 full-time and over 300 part-time vocational courses ranging from certificates to degrees (Malta Qualifications Framework (MQF) Level one to Level six).

The MCAST collaborates closely with local industries to ensure the knowledge, skills and competencies within the curricular are appropriate and relevant to a dynamic and forward-looking economy. It supports small and medium-sized enterprises through a multidisciplinary approach that encompasses work-based learning through the Apprenticeships Programme, the various entrepreneurship initiatives and through our MCAST Gateway to Industry services, whereby it provides training courses tailor-made to their needs.

MCAST Institutes and Centres

The seven MCAST Institutes provide all the technical and professional expertise towards the delivery of all programmes at MCAST with the aim of driving forward all the areas of study under their respective responsibility with an outlook towards the future. The seven MCAST Institutes are:

1. Institute of Applied Sciences.
    - Centre for Agriculture, Aquatics and Animal Sciences.
2. Institute of Business Management and Commerce.
3. Institute of Community Services.
4. Institute for the Creative Arts.
5. Institute of Engineering and Transport.
    - Electrical and Electronics Engineering.
    - Building and Construction Engineering.
    - Mechanical Engineering.
    - Maritime Institute.
6. Institute of Information and Communication Technology.
7. Gozo Campus.

1.2.3 Malta Competition and Consumer Affairs

The MCCAA was established on 23rd May 2011 with the coming into force of Chapter 510.

The functions of the Authority are the following:

- to promote, maintain and encourage competition.
- to safeguard consumers' interests and enhance their welfare.
- to promote voluntary standards and provide standardisation related services.
- to promote the national metrology strategy.
- to promote the smooth transposition and adoption of technical regulations.
- to perform such other function that may be assigned to it under this or any other law or regulations.

1.2.4 Malta Enterprise Corporation

The Malta Enterprise Corporation is the country's economic development agency, tasked with attracting new foreign direct investment as well as facilitating the growth of existing operations.

Furthermore, it acts as an adviser to Government on economic policy due to its close and constant interaction with the main economic players in the country. It is the driving force behind the creation of the Institute of Foreign Direct Investment Studies, an institution which offers research and training for foreign direct investment management to stakeholders involved in the development of foreign direct investment attraction and retention strategies. The Malta Enterprise Corporation is also the national contact point for the Enterprise Europe Network through which companies based in Malta can develop links with counterparts in over 60 other countries.

The Malta Enterprise Corporation is regulated by Chapter 463 of the Laws of Malta entitled Malta Enterprise Act.

1.2.5 Malta Freeport Corporation Ltd.

The Malta Freeport Corporation Ltd. is entrusted by Government to act as the Authority and the Regulator, at Malta Freeport. The Malta Freeport Corporation Ltd. also provides Security services at Malta Freeport.

The legislation that governs the Malta Freeport Corporation Ltd. is The Malta Freeports Act of 1989, Chapter 334.

1.2.6 Manoel Theatre

The Manoel Theatre is the official National Theatre falling under the remit of the Ministry for Justice, Culture and Local Government. The Manoel Theatreis a very important performing arts venue in Malta. A broad variety of theatrical productions in both English and Maltese languages, opera, musical recitals (including lunchtime recitals at "Sala Isouard"), poetry recitals, dramatic readings, and the annual Christmas pantomime, are performed on a yearly basis.

1.2.7 Commission for the Rights of Persons with Disability

The Commission for the Rights of Persons with Disability (CRPD) is committed to rendering Maltese society an inclusive one, in a way that persons with disability reach their full potential in all aspects of life, enjoying a high quality of life thanks to equal opportunities.

In fulfilling this mission, CRPD works in order to eliminate any form of direct or indirect social discrimination against persons with disability and their families, while providing them with the necessary assistance and support.

The Commission for the Rights of Persons with Disability is governed by Chapter 413 Equal Opportunities (Persons with Disability) Act.

1.2.8 Refugee Commission

The Office of the Refugee Commissioner within the Ministry for Home Affairs and National Security, is responsible to receive, process and determine applications for international protection in Malta, as stipulated by the Refugees Act, Chapter 420 of the Laws of Malta and its subsidiary legislation.

The fundamental objective of this Office is to ensure a totally transparent and efficient determination process while, at the same time, guaranteeing the best quality possible regarding the hearing, examination and determination of application for international protection.

1.2.9 Regulator for Energy and Water Services

The REWS was established by the House of Representatives on 31st July 2015, through the Regulator for Energy and Water Services Act (Act XXV) of 2015. The REWS is responsible for the regulation of energy and water services in Malta, whilst Article 5 of the Regulator for Energy and Water Services Act further describes the functions of the Regulator. The main business processes refer to the issue of Authorisations/Licences to the operators regulates under the Act.

1.2.10 WasteServ Malta Ltd.

WasteServ Malta Ltd. was established in November 2002 and is responsible for organising, managing and operating integrated systems for waste management including: integrated systems for minimisation, collection, transport, sorting, reuse, utilisation, recycling, treatment and disposal of solid and hazardous waste. The company also operates integrated systems for export of waste to destinations outside the Maltese islands.

Furthermore, WasteServ Malta Ltd. is also committed towards educating the general public and encouraging people to make waste management an integral lifestyle practice.

1.3 Audit Considerations

Although all the Entities are and will be exposed to a level of Cyber Security risk, the NAO is aware that such risk may vary depending on the nature of the Entity's work, the type of data being held, and the size of the Entity in terms of the number of its employees.

The NAO is also conscious of the fact that risks may increase if the Entity is offering the possibility of teleworking to its employees. Furthermore, the NAO is aware that Government Entities vary in the IT resources available, especially in terms of human resources and is conscious of the fact that some Entities do not have an IT department and thus out-source all their IT needs or part thereof.

Such information has been collated in Table 2 below and is to be considered when comparing Entities.

1.3.1 Data Collected, Stored and used

The NAO reviewed the type of information collected, stored and processed by each Government Entity involved in this exercise. Table 1 below outlines the type of information held by each Entity in the following categories: economic, policy and regulatory, national security, program and service delivery, personal data[6] and sensitive personal data[7].

[6] As defined by the Data Protection Act Chapter 440 "personal data" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

[7] As defined by the Data Protection Act Chapter 440 "sensitive personal data" means personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life;

Government Entity	Economic Data	Policy and Regulatory Data	National Security Data	Program and Service delivery	Personal Data	Sensitive Personal Data
Malita Investments p.l.c.	✓			✓	✓	
MCAST		✓		✓	✓	✓
MCCAA	✓	✓		✓	✓	
Malta Enterprise Corporation	✓	✓		✓	✓	
Malta Freeport Corporation Ltd.		✓	✓	✓	✓	
Manoel Theatre		✓		✓	✓	
Commission for the Rights of Persons with Disability		✓		✓	✓	
Refugee Commission		✓	✓	✓	✓	
REWS		✓		✓	✓	
WasteServ Malta Ltd.		✓		✓	✓	

Table 1: Data Stored, Collected and Used

1.3.2 Number of employees

The staff complement amongst the 10 audited Entities varies considerably. Although, Cyber Security risks are common for small, medium and large organisations, the negative effects of Cyber Security incidents often commensurate with the size of the organisation. The Table 2 below depicts the number of employees working within each Entity.

Government Entity	Full-Time	Part-Time	Self-Employed/ Contractors
Malita Investments p.l.c.	3	-	-
MCAST	672	160	-
MCCAA	126	9	7
Malta Enterprise Corporation	130	-	-
Malta Freeport Corporation Ltd.	84	-	-
Manoel Theatre	18	1	3
Commission for the Rights of Persons with Disability	20	3	-
Refugee Commission	26	-	-
REWS	32	-	-
WasteServ Malta Ltd.	86	12	452

Table 2: Number of Employees

1.3.3 Teleworking Arrangements

A number of Government Entities have embraced the increased use of mobility through teleworking options by offering their employees greater flexibility and an increased work-life balance.

Such teleworking arrangements, especially those related to a bring-your-own-device (BYOD) policy, or in which employees are connecting to their office network remotely from their home or public Wi-Fi, could potentially result in increased exposure to security risks. Many data breaches occur on devices used for teleworking, as they are more prone to malicious attacks.

The NAO has thus enquired about the number of employees that have been granted teleworking arrangements and recommends that such Entities have a stronger control over the personal, sensitive and/or confidential data that can be accessed by or stored on teleworking devices. The Table 3 below lists the number of teleworkers in each Entity, the hardware provided to such employees for teleworking purposes and whether such employees were provided with a secure Virtual Private Network (VPN) connection. Furthermore, this table details whether physical files are being taken out of the office by teleworkers.

Government Entity	Teleworkers	Accessed by teleworking employees	Hardware Provided	VPN connection	Physical Files being taken out of the office
Malita Investments p.l.c.	2	Network files	Laptop	Yes	No
MCAST	5	Network Files, Students Records Systems.	Laptop only in 2 cases	No	Yes in certain cases
MCCAA	28	Access folders on server, Complaints handling system.	Laptop	Yes	No
Malta Enterprise Corporation	10	E-mails, MIS/CRM	Laptop	Yes	No
Malta Freeport Corporation Ltd.	1	E-mail	Laptop	No	Yes
Manoel Theatre	2	Accounts Software, e-mail	Laptop	Yes	No
Commission for the Rights of Persons with Disability	2	Various databases, e-mail	Laptop	No	No
Refugee Commission	2	E-mail	Laptop	No	Yes
REWS	0	-	-	-	-
WasteServ Malta Ltd.	9	All the software used at the main office.	Laptop	Yes	No

Table 3: Teleworking Arrangements

1.3.4 In-house IT Unit or Out-Sourced IT services

Nowadays, IT can no longer be considered as an add-on to the day-to-day running of an Entity but must be seen as the core of the Entity's business process. The NAO understands that every Entity has developed its own working model, and management decisions were taken as to whether IT is dealt with entirely in-house, is entirely out-sourced or a combination of both.

The NAO reviewed the situation in each Entity to provide the necessary recommendations according to the Entity's situation. The NAO noted that five out of the 10 audited Entities, namely Malita Investments p.l.c., the Malta Freeport Corporation Ltd., the Manoel Theatre, the Commission for the Rights of Persons with Disability and the Refugee Commission have no IT department/person and all their IT requirements are being out-sourced to third party contractors. Notwithstanding this, in the case of the Malta Freeport Corporation Ltd. and the Refugee Commission, the NAO noted that the Ministry's CIO offices provide some IT support. Meanwhile, the NAO was informed that the main database used by the Office of the Refugee Commissioner is hosted at and supported by the National Statistics Office.

The MCAST have an IT department made up of eight people, whose main responsibilities include the maintenance on both the hardware and the network infrastructure and the provision of technical support on both the software applications and the hardware devices used within the Institutes premises.

The MCCAA has an IT Department, which is made up of an IT manager and another official. The NAO noted that the IT manager was employed shortly before the commencement of this audit and thus was in the process of taking stock of the IT needs. Furthermore, the NAO observed that the Ministry's CIO office nominated a person to assist the IT manager accordingly.

The Malta Enterprise Corporation has an IT department which is made up of four people who carry out all the IT support and maintenance except software maintenance on the Entity's financial system and support on its telephony system.

The REWS has a person in charge of IT who provides day-to-day support on the Entity's hardware and network infrastructure. The NAO noted that the leased multifunction printers are maintained by the local service provider, whilst any updates and technical support on Sage and Dakar software applications is provided by the respective suppliers. Similarly, the Time and Attendance Management application is supported by the local third party supplier as per the established Service Agreement. Furthermore, the support and maintenance of Firewall devices, Anti-virus software and the Video Conference system has been out-sourced.

WasteServ Malta Ltd. has an IT department that is composed of seven officers who carry out the overall IT support and maintenance on software applications and hardware devices with the exception of e-mail, the Fleet applications, the PABX, the Palm readers and the printers.

Conclusions and Recommendations

The NAO is of the opinion that each Entity should have at least one person in charge of its IT components. The NAO believes that whilst outsourcing all IT needs may apply in certain cases, the Entity involved unavoidably needs to understand its IT business requirements and be able to independently co-ordinate and evaluate the third-party services acquired.

Furthermore, the NAO suggests that the Ministry's CIO extends his/her expertise also to the Entity's falling under their Ministry's portfolio and ensure that such Entities have the knowledge and capability to take on board the recommendations listed in this report and action is taken where and when necessary.

1.4 ICT at the audited Entities

As part of the preliminary phases of such a complex horizontal audit, the NAO sought to determine the ICT infrastructure present at each of the 10 audited sites.

1.4.1 Applications/Databases

The IT software applications/databases used by each Entity are:

- Malita Investments p.l.c. use Microsoft Windows 10, Microsoft Office 365 and Sage Line 50.
- MCAST use Microsoft Windows 7, Microsoft Office 365, DAKAR (Payroll, HR, Online Leave Package), Access Dimensions, Asset Manager, Assignment Tracking System, Attendance, Moodle Learning Platform, Library Management System, Papercut Printing Accounts Software, Sharepoint, GEMS Online, Apprenticeship, Registrar, Admissions, TurnItIn Plagiarism Detection Software, SQL and MySQL. Other software applications are in use in lecture rooms as teaching resources.
- MCCAA use Microsoft Windows 8.1 and 10, Microsoft Office 2007, Sage, Structural Funds Database, Complaints Handling Systems and Dakar Payroll System.
- Malta Enterprise Corporation use Microsoft Windows 7, 8.1 and 10, Microsoft Office 2007 and 2012, Microsoft CRM, Microsoft Exchange, Management Information System, GetQualified, Invoice Tracking System, SUN Accounting System and the Dakar HR System.
- Malta Freeport Corporation Ltd. use Microsoft Windows 8.1, Shireburn Accounts, Shireburn Payroll and Microsoft Office.
- Manoel Theatre use Microsoft Windows Version 10, Microsoft Office Version 2013, Microsoft Office 365, Shireburn Payroll, Theatre Booking System, Sage, Shireburn Accounts and Palm Reader.
- Commission for the Rights of Persons with Disability use Microsoft Windows 7 and 10, Microsoft Office 365, Sketch Up, ACAD, Pyramid Payroll, Sage, Clients Database, Equal Opportunities Compliance Unit Cases Database, and the Library Database.
- The Refugee Commission use Microsoft Windows 8.1 and 10, Microsoft Office 2007, Evolis Signo Sign/2 Software, Card Studio Card Design Software, VSC Suite and Keesing Reference Database of Security Documents, Audacity, AeroFS, RefCom System and the Leica Application Suite.
- The REWS use DAKAR, SAGE Pastel Evolution, Open Text eDOCS DM, MySQL database, Fingertec (Time and Attendance), Microsoft Windows Server 2012, Microsoft Windows 7, Microsoft Office Professional 2007, Microsoft SQL Server 2012 and Microsoft Exchange Server 2007.
- WasteServ Malta Ltd. use Microsoft Windows 7, 8 and 10, Microsoft Office Version 2010 and 2013, Access Control, Krystal Financials, Shireburn Suite and SAN/Sharepoint Services.

1.4.2 Website

The NAO enquired whether the audited Entities have a website or websites.

- Malita Investments p.l.c. – www.malitainvestments.com
- MCAST – www.mcast.edu.mt
- MCCAA – www.mccaa.org.mt
- Malta Enterprise Corporation – www.maltaenterprise.com
- Malta Freeport Corporation Ltd. – www.maltafreeport.com.mt
- Manoel Theatre – www.teatrumanoel.com.mt
- Commission for the Rights of Persons with Disability – www.crpd.org.mt
- Refugee Commission – http://homeaffairs.gov.mt/en/mhas-departments/the%20office%20of%20the%20refugee%20commissioner/Pages/Refugee.aspx
- REWS – www.rews.org.mt
- WasteServ – www.wasteservmalta.com, www.reuse.com.mt

Conclusions and Recommendations

Though a website audit was not part of the scope of this exercise, the NAO noted that all Entities audited had a website however some of the sites may not be completely compliant with the relevant Government Website Policy[8]. In this regard, the NAO recommends that all Government Entities ensure that their current websites comply with such policy.

[8] https://www.mita.gov.mt/MediaCenter/PDFs/1_GMICT_P_0051_Website_v1.0.pdf

1.4.3 Use of social media

Modern technology has changed the face of external communications and social media, nowadays, has become a cost-effective means of providing real-time information and a valued resource in reaching the general public. Notwithstanding the fact that such interactive technology, may expose an Entity to public backlash, or negative comment posting it is undeniable that the benefits far outweigh the risks. Indeed technology allows the Entity to communicate effectively and to engage with its customers.

The NAO recognises the fact that a number of Government Entities have embraced social media and created their official Facebook page to enhance virtual communication and interaction with other Government departments, agencies and the general public.

During the course of this IT audit, the NAO investigated the use of social media and noted that six Entities have set up their official Facebook page/s.

MCAST has three official Facebook pages as detailed below:

- "MCAST" which has 12,675 likes.
- "MCAST, Institute for the Creative Arts" which has 5,159 likes and an average rating of 4.7 out of 5 from 70 reviews.
- "MCAST Libraries" which has 679 likes and an average rating of 3 out of 5 from one review.

The Malta Competition and Consumer Affairs Authority has two Facebook pages as detailed below:

- Malta Competition and Consumer Affairs Authority – MCCAA is the Authority's official page. This page has 803 likes and an average rating of 4.7 out of 5 from 3 reviews.
- Malta Competition and Consumer Affairs Authority (MCCAA) – The NAO was told that this is an old page and the Authority claimed that it is making efforts to have it removed. The NAO observed that this page may be misleading to the general public who may post a message on this page without knowing that this is not the official page.

The CRPD has an official Facebook page entitled "Commission for the Rights of Persons with Disability - CRPD" which had 2,164 likes and an average rating of 4.4 out of 5 starts from 22 reviews.

The Malta Enterprise Corporation has an official Facebook page entitled "Malta Enterprise" which has 3,236 likes and an average rating of 5 out of 5 stars stemming from six reviews.

The Manoel Theatre has an official Facebook page entitled "Teatru Manoel" which has 12,931 likes and an average rating of 4.8 out of 5 stars stemming from 87 reviews.

Finally, WasteServ Malta Ltd. has two official pages as per below:

- “WasteServ” which has 9,123 likes and no reviews.
- “WasteServ TREE centre” which has 165 likes. However, the NAO noted that the last post in this page dates back to the 30th of April, 2013.

Conclusions and Recommendations

The NAO is of the opinion that social media is only effective if it is kept continuously up-to-date and thus recommends that WasterServ Malta Ltd. closes their “WasteServ TREE centre” page since this seems to be no longer in use.

Furthermore, the NAO suggests that MCAST considers whether it is feasible to have three different official Facebook pages and would suggest closing off the “MCAST Libraries” page and including these posts in the “MCAST” page.

With regards to MCCAA, the NAO recommends that MCCAA persists in its efforts to close down this page and posts a message on this page stating that this is not its official page and guides the general public to its current facebook page.

The NAO is aware that a number of Government Entities are considering using Facebook and thus, the NAO recommends that prior to setting up an official Facebook page, the Entity concerned, nominates a person to maintain this page and ensure that it is continuously updated with notices and events. Ideally, the person in charge should also be in a position to reply to any messages received through this page as promptly as possible.

The NAO suggests that Facebook pages are promoted on the Entity’s website so as to maximise their use and encourage public interaction.

1.4.4 Servers and Data Storage Hardware

As part of the background study carried out during the preliminary phase of this audit the NAO sought to determine where the data of each of the Entities included in this audited was being hosted. The NAO noted that:

- Malita Investments p.l.c., MCAST and the Commission for the Rights of Persons with Disability use a cloud-based e-mail system and their other data is hosted on in-house servers.
- The MCCAA has its e-mails and network folders hosted at MITA, its Payroll hosted on an in-house server (with a plan to migrate this to MITA's hosting environment) and its accounting software hosted on an in-house server but backed up via a cloud service.
- The Malta Enterprise Corporation and the REWS host all their data in-house.
- The Malta Freeport Corporation Ltd. hosts all its data at MITA.
- The Manoel Theatre use a cloud-based e-mail server. The main software application, used by the theatre's booking office, is hosted on another cloud service, whilst the Accounting package and the working folders are stored on an in-house server. In addition, all the data stored by the Accounts and Administration departments is hosted on another cloud-based service.
- The Refugee Commission has its e-mails and its office automation files hosted at MITA, its main software application hosted at the National Statistics Office, whilst its other data including data of a critical nature is being saved/replicated on a local PC server.
- WasteServ Malta Ltd. has its e-mails hosted at MITA whilst all its data are hosted in-house.

Conclusions and Recommendations

The NAO acknowledges the increasing popularity of cloud computing and understands the flexibility, accessibility and storage potential that these services offer. The NAO understands that Entities with minimal or no IT resources are tempted by the idea of having no on-site server and thus no server maintenance, backups, and other routine processes to take care of.

The NAO however points out that particular attention has to be given to binding agreements signed with such suppliers and the need to clearly identify the country hosting the Entity's data. Personal or sensitive data being hosted outside Europe would need to be declared to the Data Protection Commissioner.

Furthermore, the NAO notes that MITA's strategy (2015-2017)[9] mentions the intention of exploiting cloud-based approaches and implementing a Cloud strategy for Government.

The NAO commends MITA's initiatives in this regard, and recommends that a Cloud strategy together with a set of related directives and polices are drafted as soon as possible so as to guide Government Entities and help them choose the right Cloud services for their needs, keeping in mind the risks faced by each Entity. The NAO recommends that once this strategy is published the Ministry CIOs would provide support and offer assistance to Government Departments and Entities to follow such directives and policies emanating from such a strategy.

[9] https://mita.gov.mt/en/Documents/MITA%20STRATEGY%202015-2017.pdf

1.4.5 Personal Computers

The 10 audited Entities vary in size and thus the amount of workstations (PC's, laptops and tablets) at each Entity was documented and considered.

- Malita Investments p.l.c. has a total of five laptops including two used only for its Annual General meeting.
- MCAST has a total of 2,703 workstations.
- MCCAA has a total of 107 desktops and 116 laptops.
- Malta Enterprise Corporation has a total of 65 laptops, 45 desktops and four tablets.
- Malta Freeport Corporation Ltd. has a total of eight laptops and three desktops.
- Manoel Theatre has a total of six laptops and three desktops.
- Commission for the Rights of Persons with Disability has a total of 25 workstations.
- Refugee Commission has a total of 28 laptops and eight desktops.
- REWS has a total of 12 laptops and 56 desktops.
- WasteServ Malta Ltd. has 112 desktops and 92 laptops.

1.4.6 Local Area Network (LAN)

The NAO also reviewed the local area network infrastructure at the 10 audited Entities.

- Malita Investments p.l.c. has a 16 port switch. Workstations can be connected using a wired and a wireless connection. Secure VPN connection is available to all employees. Furthermore, the network has a raided NAS and an additional external hard-drive for backup purposes.

- MCAST's Server Room is located on its Main Campus in Paola. MCAST has two separate Internet connections; one is used solely for workstations connected within the MCAST network, whilst the other connection is dedicated to Wi-Fi network. Both connections are attached to a firewall to control all incoming and outgoing network traffic based on a set of rules, whilst remote sites are connected to these links via routers using VLAN encapsulation methods. All the servers hosted at the IT Data Centre are running in a virtual environment.

- MCCAA – The Network topology at MCCAA is an extended star where each floor has a switch which is connected to a central switch found on the second floor inside the server room.

- Malta Enterprise Corporation – The main office in Pietá is connected through a single LAN, which is segregated into different subnets according to the floor level or functionality thus enabling the control of each subnet on an individual basis. Furthermore, each offsite office is connected via another separate subnet.

- Malta Freeport Corporation Ltd. – This Entity has a 24 port switch of which 14 workstations are currently in use. The port switch is connected to the Malta Government Network (MAGNET) that is provided and maintained through a maintenance contract with MITA.

- Manoel Theatre – This Entity has a 24 port switch which connects all the connections for users in the first floor administration area. This main switch also has an uplink which is bonded to a secondary 24 port switch which is managing the newer extension of offices.

- Commission for the Rights of Persons with Disability – All workstations are connected to an in-house server hosting all the software applications, file sharing and other office essentials.

- Refugee Commission – This entity has three 24 port switches connecting all its workstations to the Malta Government Network. It also has two wireless access points which provide access to the Government network. Both networks are provided and maintained by MITA.

- REWS – All the office space is located on one floor whereby all the servers, firewalls, switches and other critical devices are locked in one server room. Whilst all the VLANs are configured on the firewall devices, each port on the switches is tagged to a particular VLAN. The NAO noted that the network devices are connected to network ports depending on the assigned VLAN. In this regard, servers are connected on ports tagged on the server VLAN, workstations are connected to ports tagged on the user VLAN, whilst the wireless access point is connected to a port tagged on the guest VLAN.

- WasteServ Malta Ltd. – All devices are connected on a flat network. Currently no VLANs reside on the network, although it is envisaged that VLANs will be implemented in the near future. Since WasteServ has multiple sites around Malta and Gozo, the main servers and connections are located at the main site in Marsascala, whilst all the remaining sites are connected to the main site through ISP Bridged VLAN connection.

Conclusions and Recommendations

As part of this exercise, the NAO sought to obtain a network diagram depicting the LAN setup at each site. The NAO noted that Malita Investments p.l.c., the MCCAA, the Commission for the Rights of Persons with Disability, and the Refugee Commission did not submit such information. The NAO recommends that all Government Entities have an updated network diagram.

1.4.7 E-mail System

During the course of this audit, the NAO noted that:

- Malita Investments p.l.c., MCAST, the Commission for the Rights of Persons with Disability and the Manoel Theatre use a cloud-based e-mail system.

- The MCCAA, the Malta Freeport Corporation Ltd., the Refugee Commission and WasteServ Malta Ltd. use the Government e-mail system that is hosted and maintained by MITA.

- Finally, the Malta Enterprise Corporation and the REWS host their e-mail in-house.

1.5 Audit Scope and Objectives

The scope of this IT audit was to analyse the implementation of IT controls, assess the ICT security and physical security, and evaluate the level of Cyber Security across the selected Government Entities. Furthermore, this audit sought to determine whether Government Entities have the necessary controls to maintain data confidentiality, integrity and reliability. The audit report identified any potential risks and made the necessary recommendations to mitigate those risks. The recommendations in this report are laid out to encourage all Government Entities to assess such recommendations in light of their own circumstances and practices.

The IT audit was divided into three different stages:

- Initially, a site-survey was conducted at each of the 10 audited Entities. These audit visits sought to gather preliminary data, survey the premises including the server room, network cabinets etc. and meet the person/s in charge of IT or the person/s nominated by the auditees in the absence of IT personnel.

- Subsequently, the NAO sent an audit questionnaire to each of the 10 audited Entities to gather the necessary information. Every Entity was given the opportunity to forward parts of the questionnaire to third party suppliers in charge of their IT operations. A number of meetings were also held to help some auditees with collating the necessary information.

- The third and final stage of this audit involved the review of the data collected, the verifications of IT policies, user manuals etc. A number of on-site visits were scheduled with the auditees as deemed necessary, so as to verify the data collected. During this IT audit, the NAO also looked into the physical and logical access controls, adherence to policies, standards and procedures, network infrastructure, security controls and for any Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) that exist.

Therefore, the objectives of this report were to:

- Document all the information collected during site visits and meetings with key stakeholders and officials.

- Summarise the documentation collected and elicit the area/s of concern.

- List all the recommendations to mitigate those risks.

- Draft a set of recommendations that could be followed up and implemented across all Government Entities and not just for the 10 Entities selected for the purpose of this IT audit.

1.6 Audit Methodology

In order to attain the above objectives, a pre-audit questionnaire was sent to the 10 audited Government Entities and a number of interviews were held with key officials in each Entity.

Reference was also made to the Control Objectives for Information and related Technology (CoBit) set of best practices. CoBit is a comprehensive set of resources that contains all the information organisations need, so as to adopt an IT governance and control framework. CoBit provides good practices across a domain and process framework in a manageable and logical structure to help optimise IT-enabled investments and ensure that IT is successful in delivering against business requirements. The controls that were considered during this audit are listed in **Annex A**.

1.7 Structure of the Report

The audit report comprises of seven further chapters, each documenting the information collected and highlighting the finding and recommendations. The Recommendations under each heading are drafted in such a way that can be followed up by all Government Entities and not just by the ones being audited in this exercise.

- **Chapter 2** analyses Data Management and Data Governance, and evaluates the measures implemented to maintain confidentiality, integrity and availability of data. Furthermore, this chapter also covers the aspect of data retention.

- **Chapter 3** evaluates the measures adopted to increase user awareness towards Cyber Security and reviews the support structures available to users in terms of training, user manuals and policies.

- **Chapter 4** reviews the level of malware protection including the use of an appropriate Anti-virus software, the management of patches and the use of portable storage media devices.

- **Chapter 5** analyses the Entity's BCPs and DRPs and evaluates the likeliness of data recovery.

- **Chapter 6** reviews asset management including the IT hardware and software inventories, the physical security and the server and network monitoring.

- **Chapter 7** evaluates the access controls in place at each Entity including physical access, password management and user authentication.

- **Chapter 8** lists all the management comments submitted by the 10 audited Entities.

1.8 Acknowledgements

The NAO would like to express its appreciation to all the staff within the 10 audited Government Entities who were involved in this audit, including the Ministry's CIO and the staff within the respective Office of the CIO, for their time and assistance.

Chapter 2

Data Management and Data Governance

Chapter 2

Data Management and Data Governance

Data management, including data governance, provides assurance of data integrity throughout the data lifecycle, i.e. Data management is the business of regulating the processes that obtain/generate data, access it, process it, report upon it, store it and finally discard it at the end of the retention period.

Throughout this Chapter, the NAO sought to examine the existence and use of the below factors in the audited Government Entities under review:

- Audit Trails.
- Information Classification Policies.
- Data Retention and Storage Policies.
- Hardware disposal practices.
- Unauthorised access controls.

2.1 Audit Trails

Auditing is an important feature in an identity and access management process as it provides the necessary trail to explain who, what, when, where and how resources are accessed across the network. Auditing enables future accountability for current actions, deters users from engaging in inappropriate actions and can be used to investigate suspicious activity.

During the course of this audit, the NAO sought to establish whether the 10 Entities involved in this exercise have audit trails in place on their applications and servers. The NAO was informed that:

- Malita Investments p.l.c. mainly use Sage Accounting software upon which the full audit trail is enabled. However, this Entity does not have an audit trail mechanism set on its data server.

- MCAST disabled the audit log features on the Dakar HR/Payroll system and on the Access Dimensions. On the other hand, the audit trail mechanism is enabled on their servers.

- The MCCAA has an audit trail mechanism in place on its Complaints Handling System and its Accounting system. This Entity, however, does not have an audit trail enabled on its servers.

- The Malta Enterprise Corporation has audit trails in place on all its software applications and its servers.

- The Malta Freeport Corporation Ltd. has no audit trails in place.

- The Manoel Theatre has audit trails on its Accounting system but does not have any audit trail on its Ticketing system or on its servers.

- The Commission for the Rights of Persons with Disability does not have an audit trail in place on any of its Ms Access Databases but has an audit trail mechanism implemented on its server.

- The Refugee Commission has a basic audit trail in place on its main application, which records all changes done upon the data, who modified it and the date when these changes were made. It also has an audit trail mechanism enabled on its server.

- The REWS has audit trails in place on its Accounting and Payroll software applications. Furthermore, audit trails were also implemented in the Microsoft Access databases developed in house. Audit trails were also being kept for its servers.

- WasteServ Malta Ltd. has audit trails enabled on all its major software applications and event tracking is enabled on its server.

Conclusions and Recommendations

The NAO recommends that Government Entities implement audit trail mechanisms on their software applications and servers to the fullest possible potential. This can be done by having senior executives certifying the existence and completeness of audit trails on the software applications being used by their section/s or in the case of servers such audit logs should be certified by the person in charge of IT within the respective Government Entity.

Log events in an audit logging program[10] should at minimum include:

1. Operating System(OS) Events:
   - Start up and shut down of the system.
   - Start up and shut down of a service.
   - Network connection changes or failures.
   - Changes to, or attempts to change, system security settings and controls.

[10] Source: NIST SP 800-92, Guide to Computer Security Log Management

2. OS Audit Records:
    - Log on attempts (successful or unsuccessful).
    - The function(s) performed after logging on (e.g., reading or updating a critical file, software installation, etc.).
    - Account changes (e.g., account creation and deletion, account privilege assignment, etc.).
    - Successful/failed use of privileged accounts.

3. Application Account Information:
    - Successful and failed application authentication attempts.
    - Application account changes (e.g., account creation and deletion, account privilege assignment, etc.).
    - Use of application privileges.

4. Application operations:
    - Application startup and shutdown.
    - Application failures.
    - Major application configuration changes.
    - Application transactions, for example:
        - E-mail servers recording the sender, recipients, subject name, and attachment names for each e-mail.
        - Web servers recording each Uniform Resource Locator (URL) requested and the type of response provided by the server.
        - Business applications recording which financial records were accessed by each user.

The details logged for each event may vary widely, but at minimum each event should capture:

- Timestamp.
- Event, status, and/or error codes.
- Service/command/application name.
- User or system account associated with an event.
- Device used (e.g. source and destination Internet Protocols (IPs), terminal session identification (ID), web browser, etc.).

Furthermore, the NAO highlights the importance of using such audit trails so as to periodically monitor activity and investigate any suspicious logs. This can be done by identifying a person/s responsible for monitoring audit trails and keeping a log of when an audit trail was reviewed etc.

2.2 Information Classification Policy

Information classification is one of the initial steps in data management and basically consists of the categorisation of data. Data classification is essential in ensuring that all the officers within an Entity treat the same piece of data in a similar way.

Data classification can thus be deemed as the assignment of an economic value to intangible data and a structured approach towards data management. Moreover, data classification is fundamental to asset management, and is the basis for protecting the confidentiality of data and minimising the risks of mishandling data, including unauthorised destruction, modification or disclosure, which could lead to legal repercussions.

An Entity's Data Classification policy should:

- Define security levels for data based on the sensitivity, value and criticality of the data. A typical set of security levels may comprise the following:
    - **Top Secret** – Data and material, the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of Malta, the European Union (EU) or one or more of its Member States.
    - **Secret** – Data and material, the unauthorised disclosure of which could seriously harm the essential interests of Malta, the EU, or one or more of its Member States.
    - **Confidential** – Data that is confidential by nature and could result in a significant impact on the Entity or the Government if disclosed, modified or destroyed in an unauthorised manner.
    - **Restricted** – Data and material that is restricted and the information asset owner may only disclose it to a particular named persons/roles, on a need-to-know basis.
- List the principles that need to be followed to protect data (depending on the security level assigned to it).
- Stipulate the manner through which one can disclose data (depending on the security level assigned to it).
- List the people/Entities to whom this data may be disclosed to (depending on the security level assigned to it).
- List the procedures to be followed when disposing of data (depending on the security level assigned to it).

Conclusions and Recommendations

In this regard, the NAO noted that only one out of the 10 audited Entities (namely the Malta Enterprise Corporation), had a Data Classification policy as part of its Information Security Policy. Thus, the NAO recommends that all Entities draft their own policy in this regard and implement a Data Classification framework.

2.3 Data Retention and Storage Policy

The Data Protection Act (Cap 440)[11] specifically states that the Data "*controller shall ensure that personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed*." Government Entities are however also regulated by the National Archives Act (Cap 477)[12], which requires them to keep records for archives purposes.

The NAO noted that only one out of the 10 audited Entities (namely the Malta Enterprise Corporation), has a formal procedure in this regard. At the time of the audit this procedure was still being reviewed and hence was not being implemented.

Conclusions and Recommendations

The NAO recommends that all Public Entities:

- Establish a set of retention periods depending on their business requirements.
- Draft a Data Retention policy and distribute it to all staff. This policy should also be made available to data subjects, should it be requested.
- Draft a set of procedures detailing how the data retention requirements emulating from the policy are to be followed.
- Decide on the best way/s to dispose of their records.
- Obtain approval from the National Archivist, as necessary.

The NAO also recommends that all Government Entities follow the Government's HR retention policy with regards to their HR data. This policy was issued by the former Public Administration Human Resource Office (PAHRO), today known as the People and Standards Division, in conjunction with the National Archives, who endorsed this policy, in line with the provisions of the National Archives Act and the Commissioner for Information and Data Protection. Further information on this matter can be retrieved from the People and Standards Division website[13].

[11] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8906&l=1

[12] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lomitemid=8943l=1

[13] http://opm.gov.mt/en/PSD/PSW/Pages/PSMC/Chapter 7/Chapter-7-6.aspx

2.4 Hardware Disposal

During the course of this IT audit, the NAO reviewed the procedures adopted by the 10 audited Government Entities, for the disposal of IT equipment that is either obsolete or beyond economical repair.

The NAO noted that with the exception of Malita Investments p.l.c., who has never dealt with hardware disposal, the majority of the audited Entities have a procedure in place through which such equipment is passed on to a Board of Survey to authorise its disposal. The NAO also noted that in the case of Malta Freeport Corporation Ltd. and MCCAA, such IT equipment is sent to the Ministry's Information Management Unit (IMU), whilst the Manoel Theatre and the Commission for the Rights of Persons with Disability stated that such equipment is taken to a Civic Amenity site for recycling. Furthermore, three out of the 10 audited Entities stated that hard-disks are formatted prior disposal.

Conclusions and Recommendations

The NAO recommends that the disposal of IT equipment is treated differently from the disposal of other items, such as the disposal of slow value furniture items. The disposal of computer equipment[14] that is of a storage media nature, or contains parts which can be considered as storage media, cannot be simply thrown away.

In order to protect the Entity's data, all storage devices must be properly erased before being disposed of. It must be noted, that deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, all data, including all files and licensed software, must be removed from such equipment using a data-wiping tool prior its disposal. Furthermore, hard-drives are to be removed and rendered unreadable (by magnetising, drilling, crushing or using other effective demolition methods) prior to their disposal.

The NAO recommends that after the latter procedure is completed, a sticker or another mark is placed on the equipment indicating that disk sanitising was successfully performed. This sticker should include the date and the details of the person who performed this operation. In the case of computer equipment with non-functioning memory, this should be physically destroyed.

The Board of Survey authorising the disposal of such equipment, should not do so without having satisfactory assurance that data wiping as outlined above has been performed.

The NAO also recommends that in the case of Government Entities which may not have the technical knowledge to deal with hardware disposal or resources to perform data sanitising, discussions should be held with the respective Ministry's CIO, so as to be able to get the necessary assistance from the Ministry's IMU.

Government Entities should also ensure that IT inventories are updated accordingly to reflect such disposal of hardware.

[14] Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

Chapter 3

User Education and Awareness

Chapter 3

User Education and Awareness

A crucial element in managing cyber security is the ability of building security awareness throughout an organisation. Users are definitely the weakest link in the security stack; therefore, building an understanding amongst an Entity's employees/users of why security is important and what their responsibilities are, is a crucial component of protecting an organisation's data and IT assets.

User education can be achieved by:

- Issuing user security policies that describe acceptable and secure use of an Entity's ICT systems including Internet and e-mail usage policies, web filtering policies etc.

- Providing regular training on the cyber risks that users face in today's climate of social engineering, malware scams, and other targeted attacks. Training needs to target all levels of the organisation and should stem from informing the end users on password security and phishing risks to educating higher management on the threats and risks faced by the particular Entity. End users that come in contact with personal or sensitive data held by the organisation need to be given specialist training in this regard.

- Having user manuals as a complement to other forms of training, documenting the operation of software applications and providing an easy way for the end users to find a solution.

3.1 Training Programme

A vital part in the success of an Entity is the training given to its employees. Training gives employees the necessary knowledge and skills to carry out their work, operate effectively, increase productivity and be efficient.

There are several types of training programmes that can be used to familiarise an employee with a new role within an Entity, such as orientation sessions, induction courses, on-the-job training, and attendance to third party courses.

During this audit, the NAO sought to determine whether the Entities audited had a structured training programme or whether training was given on ad-hoc basis. Furthermore, the NAO investigated the type of training generally given i.e. whether specific in-house job training, generic in-house training or external training was provided.

The NAO noted that all the Entities concerned provided some form of training to their new employees although none of the Entities had a structured and documented training programme. Furthermore, the NAO noted that whilst all the Entities offered their employees specific on-the-job training, only two Entities (namely, the Malta Enterprise Corporation and the REWS) conducted training when a new system was developed. Although the NAO understands that the latter type of training may not apply for small Entities, with minor investment in their IT infrastructure, this form of training is to be commended, as it gives the employees the opportunity to be part of the project. In this scenario, employees could discuss and solve issues prior to the implementation phase, whilst ensuring the smooth running upon the deployment of such a new system.

Moreover, the NAO also noted that none of the Entities had a structured induction training programme for new employees and such information was only handed over through on-the-job type of learning and in an unstructured manner.

Conclusions and Recommendations

The NAO recommends that all Government Entities have a formal documented training strategy that includes a training programme catering for the needs of for each role within the organisation. This training programme should include a:

- Structured orientation/induction course to cater for new employees.
- Role specific training programme for new employees may be carried out in the form of on-the-job training.
- Training programme for employees who need to refresh their knowledge and update themselves with changes to legislation and other aspects.
- Role based training structure to form part of an employees' career progression or upon his/her appointment to a new role within the Entity.

3.2 User Manuals

User manuals support training and provide users with on-going help, comfort and confidence in using a software application.

The NAO is aware that user manuals are generally provided with off-the shelf packages but are harder to find for tailor-made software commissioned by an Entity or tailor-made software built in-house. The NAO is also aware of the fact that very often user manuals are viewed as an unnecessary cost and unpleasant reading for users. The NAO maintains that a user guide is especially beneficial for new employees who would need to fulfil a role with a minimal level of handover from their predecessor. User Manuals are especially of benefit to in small Entities where an employee may not have the option of asking a colleague for assistance and would thus need to follow such manuals to sort out any on-the-job issues.

The NAO noted that 50% of the Entities included in this audit did not have any user manuals. On the other hand, the NAO commends the other Entities namely, the Malita Investments p.l.c., the Malta Enterprise Corporation, the REWS, MCAST and WasteServ Malta Ltd. for drafting their own user manuals.

Conclusions and Recommendations

The NAO opines that when considering the purchase of a new software application due importance should be given to the availability of updated software manuals. Moreover, the NAO believes that products having an online documentation and interactive help features that would offer the user the possibility of finding the needed information rather than going through user manuals, are to be favourably considered.

Furthermore, the NAO affirms that user manuals must be easily available and accessible to employees and not kept under lock and key in offices. Entities should also consider scanning such manuals and making them available on the Entity's Intranet or accessible through the Entity's server.

The NAO also suggests that Government Entities should draft their own set of user guidelines for software applications, which did not come with the manual. In this regard, all user documentation needs to be kept up-to-date and amended every time an enhancement is carried out on the software in question.

3.3 Internet and E-mail usage policy

The NAO considers Internet and e-mail services as mission critical services and principal vehicles for electronic communications both internally within each Government Entity, as well as externally with customers, service providers, or other Government Entities. The NAO was informed that almost every employee within the 10 audited Entities under review has an e-mail account and Internet access provided by the Entity.

During the course of this IT audit, the NAO noted that the e-mail and Internet services at four of the audited Entities (namely the MCCAA, WasteServ Malta Ltd., the Refugee Commission and the Malta Freeport Corporation Ltd.) are being provided by MITA through the Government's communications backbone, the MAGNET. In this regard, the NAO observed that these Entities adhere to the "Electronic Mail and Internet Services Directive"[15] that was issued by the former Central Information Management Unit (CIMU) in 2003. Furthermore, the NAO noted that MITA maintains the right to monitor the volume of Internet and network traffic, together with Internet sites visited. The specific content of any transaction is not monitored unless there is a suspicion of improper use. In addition, an e-mail that utilises or contains invalid or forged headers, invalid or non-existent domain names or other means of deceptive addressing, will be deemed to be counterfeit when sent through the MAGNET. To this effect, any attempt to send or cause such counterfeit e-mail to be sent to, or through, the MAGNET, is unauthorised.

The NAO also observed that another three Entities have developed a policy in this regard as detailed below:

- The Malta Enterprise Corporation issued a comprehensive policy entitled "Internet Usage" regulating both Internet and e-mail usage.
- The REWS has issued a policy statement regarding the usage of e-mail and Internet as part of its "ICT systems User Security Policy".
- The MCAST has developed an "E-mail Policy" and a "Network and Internet Policy".

Meanwhile, the NAO noted that Malita Investments p.l.c., the Manoel Theatre and the Commission for the Rights of Persons with Disability have no policy in this regard.

The NAO noted that Malta Enterprise Corporation is backing up users' offline mailboxes (.pst files). This action is commendable.

[15] https://mita.gov.mt/en/GMICT/GMICT%20Policies/CIMU_D_0010_Electronic_Mail_and_Internet_Services.pdf

Conclusions and Recommendations

The NAO recommends that all Government Entities should develop and issue a policy in this regard. The policy should stipulate that:

- The e-mail service is provided for official business use only and is deemed to be the property of the respective Government Entity. Thus, an e-mail, including attachments, that is created, sent, received or printed via the Entity's e-mail service, becomes the property of that Entity.

- The personal use of e-mail is allowed only in extremely exceptional cases and provided that this does not interfere with the performance of the user's duties or the integrity of the Entity.

- Every user is responsible and held accountable for his/her Internet activities and is duty bound to prevent access to illegal material.

- Users are expected to use the Internet productively and in connection with job-related activities. The personal use of the Internet service must be infrequent and must not interfere with the duties of the employee or compromise a security risk to the Entity.

The NAO suggests that Government Entities issue periodical reminders to all e-mail and Internet users, highlighting the salient points in the "Electronic Mail and Internet Services Directive". In particular, reference should especially be made to, the restrictions on the use e-mail and Internet services as reproduced in **Annex B** and the user responsibilities in connection with mailbox maintenance.

Furthermore, the NAO is of the opinion that Government Entities should discuss the possibility and feasibility of having offline mailboxes saved on network drives and backed up regularly. This discussion may be held with the respective Ministry's CIO, keeping in mind the genre of the correspondence being carried out through e-mail by that particular Government Entity or by certain users within that Government Entity. The NAO recommends that wherever this is not possible, users are to be made aware that offline mailboxes are stored on the PC's hard-disk drive, and thus should something happen to the PC, this correspondence may be lost. A Government Entity should thus suggest that such mailboxes are backed up by the user.

3.4 Web Filtering Policy

A web filter is a program that can analyse a website and determine whether some or all of it should be displayed or not to the user. The web filter can be practically compared to a sieve which allows the legitimate data to pass through the filter whilst stopping unwanted or bad data.

The web filter works by checking the origin and content of a website against a set of pre-configured rules, and accurately pinpointing a portion or portions of a web page which should not be allowed into the internal network. This may include web pages that include objectionable advertising, pornographic content, spyware, viruses and other offensive content.

MITA, being the Government Internet service provider, has adopted the "Web Filtering Directive"[16] that was issued by the former CIMU in 2003. The aim of this directive is to set up methods for controlled access to Internet websites based on Government needs. The directive addresses the:

- Legal risks to Government – The liability of inappropriate content.

- Security risks – The risks to the Entity's hardware, software and network, and the security risks posed upon the entire MAGNET.

- Productivity issues – The loss of employee productivity due to Internet abuse.

The web filtering can be configured to either 'white-list' or 'black-list' a website. Only websites found in the 'white-list' group can be accessed when 'white-list' is enabled. On the other hand, if 'black-list' is enabled, the web filter will allow all websites except those listed in the 'black-list'. In the event that a particular website is being blocked or needs to be blocked by the web filter, the respective IT Unit will liaise with MITA's Service Call Centre to take the necessary action to 'white-list' or 'black-list' the website accordingly.

During the course of this IT audit, the NAO noted that:

- Three audited Entities (namely Malita Investments p.l.c., the Manoel Theatre, and the Commission for the Rights of Persons with Disability) have no web filtering policy and no website filtering was implemented.

- Three audited Entities (namely the MCCAA, the Malta Freeport Corporation and the Refugee Commission) are using the web filtering services offered by MITA as detailed above.

[16] https://mita.gov.mt/en/GMICT/GMICT%20Policies/CIMU_D_0014_Web_Filtering.pdf

- The REWS does not have a web filtering policy, although filtering was implemented through a firewall.

- The MCAST have a web filtering policy and are make use of a web filtering tool.

- WasteServ Malta Ltd. have enacted a web filtering policy, however, it is unclear whether the Internet service at this site was being filtered or not.

- The Malta Enterprise Corporation has a policy, furthermore Internet at this site is being filtered at the router level allowing data destined to approved ports and filtered by URL requests.

Conclusions and Recommendations

The NAO recommends that all Government Entities install a web filter and configure it to block illegal content, or any content, which is objectionable or can contribute to the loss of productivity. The list of websites that needs to be blocked should be compiled according to the Entity's needs. Government Entities may also wish to consult their Ministry's CIO to implement an effective web filtering solution.

3.5 User Awareness of Cyber Risks

The protection of Government Information Systems is a key responsibility of all Government Entities, having regard to each Entity's business operations and specific risks. In the context of a national Government, those risks can range from threats to national security through to the disclosure of sensitive personal data.

According to the "*IBM X-Force® Research 2016 Cyber Security Intelligence Index*"[17] unauthorised access was the leading cause of cyber security incidents in 2015, accounting to 45% when compared to 37% in 2014. Furthermore, this research also states that 60% of all attackers are stemming from "insiders", i.e. people who work for the organisation, such as employees, contractors and consultants. Insider 'attacks' have been noted to be some of the most dangerous, since employees are already quite familiar with the Entity's infrastructure.

During the course of this audit, the NAO sought to determine whether the 10 audited Entities are providing security awareness training to their employees. The NAO positively noted that the Refugee Commission started an IT Awareness campaign, provisioned by the Office of the CIO. Likewise, Malita Investments p.l.c. and the Commission for the Rights of Persons with Disability stated that security awareness is provided to their employees. It was however unclear whether all employees were being targeted, and whether such measures involved awareness training or just reminders/posters highlighting some threats. In the meantime, the REWS and MCCAA stated that e-mails are occasionally sent to all users informing them about new threats, whilst the MCCAA also displays such information on the Entity's notice board. On the other hand, WasteServ Malta Ltd. commented that whilst such training is not provided, users are notified individually when new threats are identified.

Furthermore, the NAO noted that most of the Entities under review, are relying on policies to convey their message. Whilst the NAO commends structured policies stipulating what is considered as misuse, on the other hand it stresses that such policies should not replace the need for training.

Conclusions and Recommendations

The NAO acknowledges that some of the best ways for an Entity to improve Information Security are by raising awareness through the provision of information about the basics of Information Security, and providing training and educating everyone who interacts with its computer network and the Entity's systems.

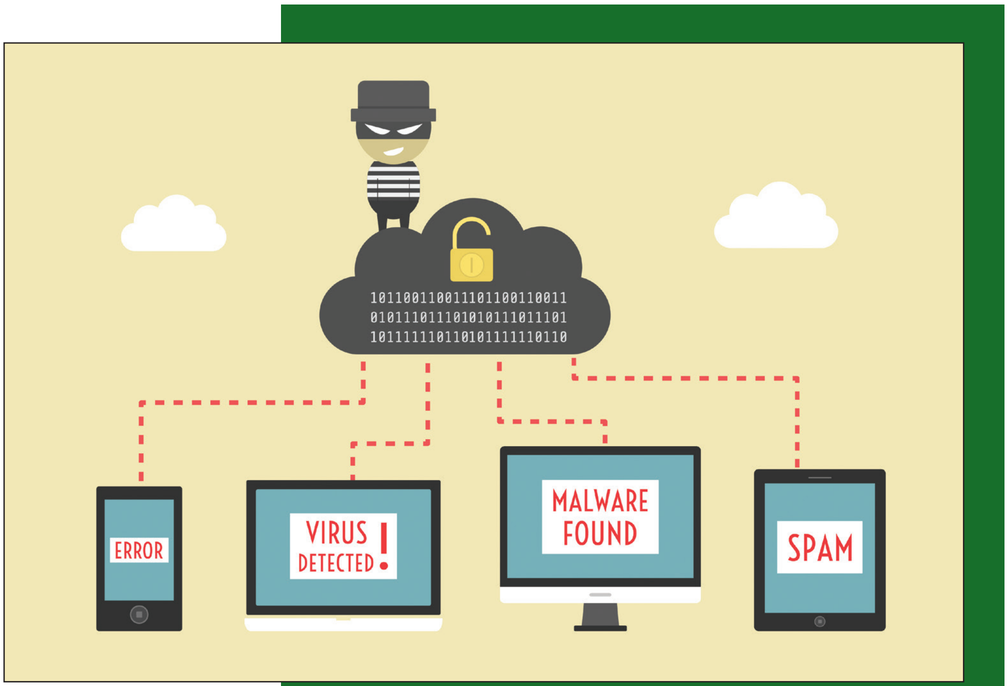
The NAO therefore recommends that such training is offered as part of the induction sessions given to new employees. This training should also be part of an ongoing programme, that seeks to ensure that all users are familiar with Information Security policies and best practices that govern the use of

[17] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF

IT assets. Awareness on Security policies and best practices is normally communicated through the use of e-mails, published leaflets, handbooks or verbal communications, to ensure that information is conveyed to the appropriate users in a timely manner. In this regard, it would be good standard practice if employees were reminded periodically about:

- The importance of backing up important files, folders and offline mailboxes.
- How to avoid phishing, not to open any executable files or any suspicious attachments, and not to subscribe to unnecessary or unverified mailing lists.
- The importance of using strong passwords.
- Safeguarding passwords and user accounts and prohibiting the sharing of logins and passwords.

In this regard, the NAO recommends that Government Entities encourage their employees to attend the “Information Security Awareness” course, which is offered from time-to-time by the Government’s former Centre for Development, Research and Training (CDRT), now referred as the Institute for Public Services (IPS) in Floriana. The objective of this course is to raise awareness among the participants regarding the pitfalls that could be encountered when handling information. Nowadays, most of the information is in electronic format, which is retained on computers that are networked to facilitate access. This means that the need to keep the information safe and secure is even more important. The course covers real-life cases on Information Security incidents and various other topics that include, amongst others, malware, password use, surfing the net, e-mail use, protection of data, social engineering and networking, mobile devices, Wi-Fi, physical security and incident management.



Chapter 4

Malware Protection

Chapter 4

Malware Protection

The exchange of information carries a degree of risk as it could expose the Government Entities to malicious code and malware, which could seriously damage the confidentiality, integrity and availability of data and the technologies on which it is hosted.

Malware can attack any system and thus the adoption of a defensive security architecture is a must. The following controls are considered essential to manage the risks from malware:

4.1 Anti-Virus Software

All Government Entities are expected to deploy an adequate anti-virus software that would scan all inbound and outbound traffic on its internal network and on host systems.

During the course of this audit, the NAO assessed whether the Entities being audited had an anti-virus installed on their workstations and their servers. The NAO was pleased to note that all the Entities audited had an anti-virus that was being updated regularly.

The NAO however noted that some PC's were at times disconnected from the internal network as users opt to use a separate Wi-Fi network connection or in view of teleworking arrangements. In both cases such desktops or laptops would therefore not be updated anti-virus definitions, posing a risk to the Entity concerned.

The NAO noted that Malta Enterprise Corporation monitors the status of anti-virus definitions and any malware activities on its computers, electronically.

Conclusions and Recommendations

Taking into consideration the above observations, this Office recommends that all Entities issue a periodic report (e.g. every six months), to verify that all computers are being updated with the latest anti-virus definitions.

4.2 Patch Management

With the rise of malicious code targeting known vulnerabilities on un-patched systems and the resultant negative affects incurred by such attacks, patch management has become a pivotal process within an organisation's list of security priorities.

The key role of a successful patch management strategy is to help improve security without disrupting business critical systems. This is achieved by enforcing a consistently configured environment that is protected against known vulnerabilities, in both operating systems and application software.

Operating system manufacturers usually provide regular product updates. These are classified as security or critical updates to protect against vulnerabilities to malware and security exploits. Security updates are routinely provided by the manufacturer on a monthly basis, or can be provided whenever a new update is urgently required to prevent a newly discovered or prevalent exploit targeting Microsoft Windows users.

During this IT audit, the NAO reviewed the patch management framework adopted by each Entity on their workstations and on their servers. The NAO noted that most of the Entities audited did not appreciate the importance of patch management and were under the false impression that their anti-virus software would protect them against all threats. This is not only dangerous but it entirely incorrect.

In this scenario, an anti-virus software is NOT capable to protect from faulty code in approved applications. It is only patches that are designed to fix bad code; also referred to as bugs. This bad code could be a mistake made by a programmer, or an incompatibility with another piece of software. When that mistake can be exploited by an attacker, patching that code is the only way to prevent the vulnerability from being exploited. In simple terms, an anti-virus software is similar to having a security guard, and patches can be seen as having adequate locks. Whilst, the security guard (anti-virus) can react to the presence of a thief, it is only the presence of adequate locks (patches) that could proactively keep the thief completely out of the system. Using both will help to bolster ones defences and is a good start towards having a thorough and effective protection against threats.

Patching is an on-going task, with both monthly releases from the major operating system vendors and unpredictable releases from software vendors as new vulnerabilities are discovered. It is thus imperative that Entities ensure that all the necessary patches are installed on all the systems that require them. The best way to accomplish this is by using patch management software, which is a centralised application that automatically deploys patches to every system on the network. Such software may make it possible to test such patches and roll back any patches that turn out to have their own problems. The NAO however understands that procuring a patch management software may not be feasible for all Entities and in such cases, operating systems are to be updated automatically, whilst other patches are to be rolled out as quickly as possible.

The NAO noted that:

- The MCCAA, and the Malta Enterprise Corporation have a patch management software.
- The Refugee Commission has its patch management managed by a third party supplier.
- MCAST, the REWS and WasteServ Malta Ltd. have set their operating systems to update automatically but do not have a formal plan for the deployment of other patches.
- The Malita Investments p.l.c., the Malta Freeport Corporation Ltd., the Manoel Theatre and the Commission for the Rights of Persons with Disability have no formal plan in this regard.

Conclusions and Recommendations

The NAO recommends that all new PCs are configured to automatically download and install product updates through the Microsoft Windows update tool. All the hotfixes and patches which are released by Microsoft are distributed across MAGNET on all the Entities' workstations connected to MITA. The NAO recommends that those Entities that are not connected to MAGNET devise a formal plan as to how patch management will be dealt with and should consider the installation of a patch management software.

Furthermore the NAO recommends that those Entities that have their own servers installed on site adopt the best practice of installing hotfixes or service packs on a testing server and then deploying these patches on their live servers, if no abnormal behaviour is observed. The respective IT Unit should ensure that the server is backed up successfully, prior to installing any security or critical update. Moreover, the NAO recommends that Entities that have their servers managed by a third party supplier should ensure that patch management on such servers is being implemented as per best practices detailed above.

4.3 Use of Portable Smart Media and Storage Devices

Smart Media portable devices, that can transfer data through a wired or wireless connection, give users the convenience to access both work-related data and personal data whilst on-the-go. The NAO is conscious of the fact that the use of such devices has increased drastically in recent years and is concerned about the associated risks that these devices bring upon Government Entities.

The portability of such devices and the smart features that enable an on-the-go connection to various networks and hosts brings about a higher risk of:

- Data loss (when a device is physically lost).
- Data exposure (when personal, sensitive or commercial data is exposed to third parties without any authorisation or consent).
- Surreptitiously infecting other PCs and networks due to the lack of anti-virus software and inherently poor security tools installed on such devices.
- Network-based attacks to any system the portable device is connected to, or is authorised to connect to.

Similarly, the use of portable devices such as external hard-drives, USB memory sticks and memory cards, albeit not being able to connect these devices to a wireless network, still carry the above listed risks especially those associated with data loss, data exposure and malware exposure.

During this IT audit, the NAO enquired about the use of such devices at the Government Entities being audited. The NAO noted that personal (i.e. employee-owned) portable devices can be used in all the Government Entities under review, to access Internet and e-mail through segregated Wi-Fi connections. All the Entities audited informed the NAO that such devices are not allowed to access the internal networks. However, one should note that personal, sensitive and commercial data is also shared through e-mail, and thus accessing the Government e-mail through such devices is automatically posing a risk to the Government Entities owning that data.

The NAO also enquired whether the Entities being audited have developed a policy regulating the use of such devices. The NAO noted that the Malta Enterprise Corporation was the only Entity which had a comprehensive policy in this regard. Meanwhile, MCAST had an IT policy which mentions the use of "*personal equipment*" and prohibited such equipment from being connected to its network without prior authorisation from the IT Department. This MCAST IT policy also permits personal equipment to be connected to its Wi-Fi, however, stops short of listing the user's responsibilities in this regard.

Conclusions and Recommendations

The NAO recommends that all Government Entities:

- Inform their employees about the risks associated with using such devices.
- As far as practically possible, limit or discourage the use of personal portable storage media devices, except for those owned by the Entity and used where there is a valid business case that has been pre-approved by the person in charge of IT.
- Develop security and acceptable-use policies for all portable devices, and inform employees about such policies, their importance and the responsibilities upon each employee.
- Encourage employees to take all the necessary precautions to protect themselves against the theft of portable devices, particularly by pointing out typical scenarios including not leaving such devices unattended in a vehicle, or putting such devices in checked luggage when travelling abroad.
- Encourage employees to report any missing devices immediately both those owned by the Entity as well as personal devices which may contain the Entity's data.
- Forbid the connection of any devices to the Entity's network without the pre-approval of the person in charge of IT.
- Ensure that the Entity's network can only be accessed through a secure VPN connection.
- Evaluate the possibility of configuring Secure Sockets Layer (SSL) security features on the organisation's web servers to encrypt data being transmitted.
- Encourage employees to disable Wi-fi and Bluetooth when not in use, and set Bluetooth to "non-discoverable", to make the device invisible to unauthenticated devices.
- Encourage employees to take regular backups of the data stored on such devices.

- Consider implementing an inventory of mobile devices that are likely to carry personal, sensitive or commercial information that is owned by the Entity and audit such devices on a regular basis to:

    - Ensure that employees password protect their devices using a strong password or PIN which is changed periodically.

    - Educate the employees so as not to allow their devices to be used by other people including members of their immediate family.

    - Ensure that an anti-malware software is installed on such devices and regular scans are carried out.

    - If possible, a local firewall should be installed on the device to filter inbound and outbound traffic, and block malicious code.

    - If possible, enable a remote-wiping feature, to erase all data on the device, in the event that it is lost or misplaced.

Although the NAO is aware that such devices are nowadays considered necessary tools, this Office encourages the implementation of the best practices outlined above, so as to mitigate the risks associated with the use of such technologies, as much as possible.

Chapter 5

Disaster Recovery

Chapter 5

Disaster Recovery

Within the IT sector, disasters can take several different forms from a hard disk failure, to a power outage, a computer security exploit, floods, fires, theft, sabotage, etc. Although the randomness of some of these disasters lulls some organisations into a false sense of security – "that's not likely to happen to us" reasoning, unfortunately catastrophes do happen, with potentially extremely negative consequences.

This Chapter deals with assessing the Entities' level of preparedness towards such incidents, their plans or processes for rebuilding the operations or infrastructure, and how such Entities recover their business applications following a disaster.

5.1 Business Continuity and Disaster Recovery Plans

During the course of this audit, the NAO assessed whether the Entities under review had any Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) in place.

The primary objective of a BCP is to protect the organisation in the event that all parts of its operations and/or Information Systems are rendered unusable, and to help the organisation recover from the effects of such events. The BCP defines the roles and responsibilities of the Entity's key personnel and identifies the critical IT application programs, operation systems, networks, facilities, data files, hardware and time-frames required to assure high availability and system reliability, based on the inputs received from a Business Impact Analysis and Risk Assessment exercise.

As part of the above-mentioned BCP, an Entity should develop a DRP stipulating the procedures that are to be taken into account in the event that the IT facilities become inoperable due to extreme incidents. This plan should also document the recovery approach, the recovery time objectives and the sequence of events, including the pre-requisites, the dependencies and the responsibilities assigned to every individual involved in the plan.

During the audit, the NAO noted that none of the Entities audited had any documented plans in this regard. Notwithstanding this, the NAO noted that the Malta Enterprise Corporation has a documented set of procedures outlining the importance of such plans, and detailing the factors to be included in such plans. The Malta Enterprise Corporation has however confirmed that these procedures were not yet implemented and Management intended to create a standard framework for all BCPs, so as to have a consistent format throughout the organisation.

Furthermore, the NAO enquired whether the Entities audited have an alternative site from where to resume operations. The NAO noted that nine of the audited Entities did not have an an alternative site, however the Malta Enterprise Corporation has two locations where key people could continue operations.

The NAO also sought to gauge whether the Entities audited have a manual process in place that could temporarily maintain the operational functionality of the Entity in the event of a total IT system collapse. It was noted that none of the Entities have a clearly defined set of manual processes that could be adopted in such circumstances. However the REWS stated that its paper files could be used to get any required information, whilst acknowledgements and receipts could temporarily be issued manually so as to maintain operational functionality.

Conclusions and Recommendations

In this regard, the NAO recommends that all Government Entities should draw up a formal documented BCP and DRP, designed to reduce the impact that disruptions might inflict on the Entity's operations. (vide **Annex C**).

Additionally, when the DRP is finalised, this should be tested on a regular basis. In this regard, the key persons should familiarise themselves with the recovery process and the procedures to be followed in the event that the DRP has to be invoked. This testing process will evaluate the effectiveness of the recovery documentation and establish whether the recovery objectives are achievable. The final objective is to identify any improvements required in the disaster recovery strategy, infrastructure and the recovery processes, established in the DRP.

Apart from having a DRP, Government Entities should ensure that the SLAs with their respective suppliers cater for an adequate and timely maintenance, support and IT business continuity.

Furthermore, the NAO suggests that Government Entities reflect on the possibility of having an alternative site from where to resume operations. Whilst the NAO acknowledges the fact that this solution may not be feasible for all the Entities, the NAO suggests that this solution is analysed, especially for those Entities who are already conducting their business from multiple sites.

Moreover, the NAO commends Entities having a manual process in place, that could temporarily maintain the operational functionality of the Entity in the event of a total IT system collapse. The NAO however understands that setting up such a manual process that backs-up the electronic processing within an Entity is not always possible. The NAO encourages Government Entities to reflect on this possibility and to devise and implement a concrete plan in this regard where possible.

5.2 Backup

A sound backup plan is critical for restoring systems or applications after a disruptive event. This is especially important in view of the fact that Government Entities own and manage data that is at times sensitive, confidential and may affect the daily operation of other Government Entities and have an impact on the lives of citizens.

During this audit, the NAO examined whether data was being backed up, whether such backups were scheduled or run on an ad-hoc basis, the backup approach adopted and the media used for such backups.

The NAO noted that whilst all the Entities audited are backing up the data residing on their servers, the users within these Entities do not necessarily save their data on the Entity's server/s, with the consequence of having data stored on the hard-disk of desktop or laptop computers. The NAO noted that Entities with a prevalence of teleworking arrangements (vide 1.3.3 Teleworking Arrangements), Entities that operate from multiple sites and Entities whose business involves having employees travelling to other countries, face a greater risk of having data saved locally on computers, and not backed up.

Further to the above, the NAO enquired whether backups are scheduled or whether these are run randomly whenever it is felt necessary. In this regard, the NAO noted that all the Entities with the exception of Malita Investments p.l.c., the Refugee Commission, the CRPD and the MCCAA have an automated scheduled backup system.

Moreover, the NAO analysed the backup system used and the media upon which such backups were being performed. The NAO noted that all the Entities audited run their backups daily, with the exception of the Manoel Theatre where backups are run weekly. Additionally, the NAO observed that backups are being performed on tapes, external hard-drives, NAS devices, CD's, DVD's and pen drives. The NAO noted that one Entity performs its backups on a local PC Server. Some Entities were looking at implementing cloud data backup (remotely via Internet).

Conclusions and Recommendations

Although the NAO understands the various limitations (human, knowledge and financial) of some Entities, the NAO is deeply concerned about the lack of backup procedures and awareness on this subject, and thus recommends that CIO's provide their expertise on the ground in order to help Government Entities in this regard. Furthermore, the NAO is of the opinion that the responsibility of establishing an adequate backup procedure and the overseeing mechanism to ascertain that such procedure is being followed, should be a shared responsibility between the Entity and its Ministry CIO.

The data being held by Government Entities is Government data and thus should be treated as such to ensure confidentiality, integrity and availability of such data. Government Entities, especially those considered small in size, may not always have a safe data management and backup methodology. Thus, the CIO's should principally help in the drafting of an established and documented backup schedule for each Entity in their portfolio, and determine the person/s responsible within each Entity who will be tasked with the daily running of backups. The CIO's should also help in determining the correct backup type (e.g. incremental backups performed daily, full-backups performed weekly, monthly and yearly) and the best time of the day when such backups are scheduled (e.g. after office hours). Finally, CIO's should also take on the responsibility of ensuring that backup logs are kept by respective Entities.

The NAO deems user awareness to play a big part of an Entity's backup procedure and thus recommends that training is provided so that all personnel understand the need to adopt a backup procedure and ensure that all their important files are included in the Entity's backup procedures. The NAO is against the practice of having personnel taking ad-hoc backups when they deem necessary.

The NAO further recommends that all Government Entities implement an automated backup rotation scheme (e.g. Grandfather-father-son) with backups taken daily, weekly and monthly. In addition a yearly backup should also be done.

Whilst the NAO acknowledges that cloud computing has become very popular and understands that cloud storage gives the added advantage of having data backed up automatically and stored off-site, the NAO highlights the importance of ensuring that Government data has an adequate level of protection, to maintain data security and privacy. The NAO thus recommends that the Ministry CIOs discuss the issue of cloud computing and cloud storage with MITA and come up with a corporate government strategy (vide 1.4.4 Servers and Data Storage Hardware).

Furthermore, the NAO is of the opinion that backups on CD's, DVD's, pen drives and/or locally on PC's should be avoided at all costs. The NAO recommends that backups are performed on tapes, external hard-drives or NAS devices, by authorised officers within each Entity who will be responsible for ensuring compliance with a pre-established backup schedule and monitor the successful completion of the backup process.

5.3 Storage of Backup Media

One of the most serious mistakes commonly made relating to backups is how and where the backup files/media are stored. Most organisations are inclined to store backup media in proximity to the original source, assuming that hardware malfunction or software errors are the only types of incidents that the organisation may face relating to backups. Additionally, a number of organisations do not protect backup media from physical access, and do not store such media in secure locations.

As per best practice, an organisation should always store backups in a physically secure location, far enough so as not to be affected by the same fire, flood, or storm that might destroy data in its offices. Backup media should be stored in a non-adjoining building (if possible) that is, not prone to flooding, and away from possible sources of fire or corrosive elements. Additionally, backup media should be protected from access with the same level of protection as the working data itself and thus access should be controlled and limited to those with appropriate clearance.

During this audit, the NAO noted that only four out of the 10 audited Entities are storing their backup media off-site. Furthermore, the NAO observed that only two of the 10 Entities are storing such media in fire-resistant safes, whilst another Entity is storing its backup media in a fire-resistant room.

Conclusions and Recommendations

The NAO recommends that backup media is stored off-site. Notwithstanding this, the NAO acknowledges that the Entities concerned may only have one physical location available and thus this measure would be difficult to implement. The NAO therefore recommends that such Entities hold discussions with their respective Ministry CIOs with the aim of finding another location where such backup media could be stored, ideally in a fire-resistant safe that would only be accessible to a limited and controlled number of authorised personnel.

Moreover, the NAO discourages the practice of storing backup media in office cabinets and deems the possibility of backup media being taken home by personnel as unacceptable.

5.4 Recovery of Data

Backup data is of no use if it cannot be restored back to its normal use. It is thus important for organisations to test their backups periodically to ensure data integrity.

During the audit, the NAO enquired whether backups were being tested, and if so in which way was this being done and how often. The NAO also enquired as to whether the Entities audited have ever restored data from backup and the date when the last restore was carried out.

The NAO noted that six out of the 10 audited Entities were testing their backups, another Entity was testing some of its backups, whilst the remaining three Entities had never tested their backups. The NAO however was not provided with any evidence documenting such testing and thus could not ascertain whether such tests were actually done periodically or on ad-hoc basis.

Furthermore, upon enquiry, only five out of the 10 audited Entities stated that data restores (albeit in some cases not a full data restore) was successfully done.

Conclusions and Recommendations

The NAO recommends that all backups are to be fully restored at least once a year and such testing is documented with a screenshot showing that the data was successfully restored form backups.

Chapter 6

Asset Management

Chapter 6

Asset Management

Asset Management constitutes a set of business practices that support strategic decision making by optimising costs, making the best use of current resources, eliminating waste, encouraging redistribution and improving efficiency. IT Asset Management involves gathering a detailed inventory of an organisation's hardware and software.

This Chapter seeks to determine whether the Government Entities being audited are maintaining an IT hardware and software inventory and adopting the right measures to safeguard such assets, both in terms of physical security within the building, and in terms of server and network monitoring.

6.1 IT Inventories

The NAO acknowledges that one of the toughest tasks for IT managers and administrators is keeping track of computers, network devices and software applications. However, this is considered to be a very important task since such information would enable public Entities to keep track of their IT investments and manage these resources efficiently.

The IT audit assessed how each Entity manages and administers its IT assets, both in terms of hardware as well as software licences.

Hardware

The IT audit established that the majority (eight) of the Entities maintain some form of inventory database for IT hardware assets.

In fact, the MCCAA, the Malta Enterprise Corporation, and WasteServ Malta Ltd. are all using a specific automated system (application or module) for this purpose. However, only an extract from the MCCAA's system was made available during the course of this IT audit. Furthermore, the Malta Enterprise Corporation also maintains a detailed manual hardware inventory in Microsoft Excel, for cross-checking purposes.

Another detailed IT hardware inventory in Microsoft Excel is maintained by the REWS, and includes a unique asset number, the name of the officer responsible for the asset and various asset details, but it omits the assets' serial numbers (where applicable).

Similar IT hardware inventories in Microsoft Excel are also kept and utilised by Malita Investments p.l.c., the Malta Freeport Corporation Ltd., and the Refugee Commission[18], all of which include assets' serial numbers and to whom each asset has been allocated, amongst other details.

Meanwhile, the MCAST stated that during the course of this IT audit, a full physical count of all its IT assets was underway, with a variety of details being inputted and recorded in a new fixed asset register. Both the previous register and this new register Entity were compiled in Microsoft Excel.

Notwithstanding the above, the NAO noted that neither the Manoel Theatre nor the CRPD have an IT inventory to keep track of their respective IT hardware, although the former claimed that they are in the process of establishing such an inventory.

Software

On the other hand, the IT audit revealed that only half of the Entities reviewed were maintaining inventory records to keep track of IT software licences.

In this regard, both the Malta Enterprise Corporation and WasteServ Malta Ltd. maintain records of software licences owned using an automated system, although extracts from WasteServ Malta Ltd.'s system were not made available during the audit. Moreover, the Malta Enterprise Corporation also records the applicable software installed on each device, on manual forms which are then handed out with each respective PC/laptop.

Malita Investments p.l.c. maintains a list of software licences in Microsoft Excel, with details of serial numbers and which PC/laptop it was installed on. Similarly REWS is maintaining an inventory of software licences in Microsoft Excel.

Additionally, the Refugee Commission claimed to have adopted a software asset register, although these files/documents were not provided during the IT audit.

Conversely, this Office observed that the MCAST, the MCCAA, the Malta Freeport Corporation Ltd., the Manoel Theatre, and the CRPD do not keep an inventory of software licences owned.

The NAO further noted that any physical licence documents or certificates pertaining to the MCAST are currently kept in a specific file, whilst any similar documents relating to the Manoel Theatre currently remain filed with the respective invoices at the Entity's Accounts Department. Nevertheless, as already indicated earlier on, the latter reaffirmed that it was in the process of establishing an IT inventory.

[18] Whilst this IT inventory database is maintained in Microsoft Excel, a copy of this document was provided by this Entity to NAO in .pdf format.

Conclusions and Recommendations

In light of the above observations, the NAO strongly recommends that each of the Entities reviewed should maintain a detailed inventory of their IT hardware and software licences. Such an inventory database could be set up using basic tools such as Microsoft Excel or Access, and at the least, should include fields such as item details, uniquely identifiable item number, physical location and/or to whom this has been assigned.

6.2 Physical Security

The NAO deems physical security to be the foundation of any overall security strategy. Physical security measures are aimed to prevent a direct attack on the Entity's assets or reduce the potential damage that can be inflicted, should an incident occur.

Although not strictly within the scope of this audit, the NAO verified the following controls in place related to physical access, server room environment and fire prevention which are covered in this Section and Section 6.4 Adequacy of Server Room.

Security Measures and Systems

The audit team noted that WasteServ Malta Ltd. has a full complement of security measures and systems, comprising of an intruder alarm at its main sites in Marsascala and Magħtab, as well as closed circuit television (CCTV) cameras, security guard/s and watchmen on all its premises.

The NAO also noted that most of the Entities under scrutiny have a balanced and well rounded mix of security measures and systems. In fact, the MCAST, the Malta Enterprise Corporation, and the Malta Freeport Corporation Ltd. all have an intruder alarm, CCTV cameras and a security guard. Furthermore, the Malta Enterprise Corporation has a centralised system that controls access to the different areas within the building and its security guard is stationed at the reception desk after office hours, whilst the Malta Freeport Corporation Ltd. claimed that its intruder alarm is manned on a 24/7 basis.

During the audit, it also transpired that the MCCAA and the REWS both have an intruder alarm and a CCTV system installed on their sites, whilst the Manoel Theatre has a security guard to complement the CCTV cameras installed.

Moreover, from the feedback provided, it transpired that Malita Investments p.l.c. makes use of the services of a security guard to monitor security on its premises. The NAO noted, that the Refugee Commission has one full time Detention Security Officer and two Rapid Intervention Unit policemen who guard the entrance to the Office during reception opening hours.

Meanwhile, the CRPD admitted that it has no security measures in place or security systems installed on site.

Visitors' Policy

With regards to visitors' policies, the NAO unfortunately noted, that the vast majority of the Entities do not have any such formally documented visitors' policy in place. This statement applies to no less than eight of the Entities under scrutiny, namely, the:

- MCAST.
- MCCAA.
- Malta Enterprise Corporation.
- Manoel Theatre.
- CRPD.
- Refugee Commission.
- REWS.
- WasteServ Malta Ltd.

However, the MCAST and the Malta Enterprise Corporation stated that a procedure is in place whereby visitors have to sign a visitor's log book at the reception desk. In addition, visitors at the MCCAA and WasteServ Malta Ltd. are also provided with a temporary guest card/tag while accessing the Entity's site/s. Such visitor logging practices were also confirmed by the NAO during the site audit visits.

To this extent, the Refugee Commission and the REWS claimed that visitors are always accompanied by members of staff, whilst the Manoel Theatre added that the relevant policy is planned to be implemented. The CRPD did not provide any comments on this matter.

In the meantime, it transpired that both the Malta Freeport Corporation Ltd. and Malita Investments p.l.c. have a formally documented visitors' policy in place. However, the latter did not provide a copy of such policy to this Office for review, claiming that this is "...*held by MIMCOL the lessor of the premises*."

Smoke Detectors

During the course of the IT audit, the NAO noted that with the exception of Malita Investments p.l.c., the CRPD and the Refugee Commission, all the remaining Entities under assessment have smoke detectors installed, either in a specific area or blocks, or throughout the whole building/s.

In fact, the MCCAA, the Malta Enterprise Corporation, the Malta Freeport Corporation Ltd., and the REWS, have smoke detectors installed throughout all their building/s.

Similarly, WasteServ Malta Ltd. has smoke detectors installed at all its sites and buildings, with the exception of the public Civic Amenity Sites and Weighbridges.

In the meantime, smoke detectors at the MCAST are only installed in a number of specific areas/blocks, whilst such devices are only installed at the theatre within the Manoel Theatre.

On the other hand, no smoke detectors are placed within buildings occupied by the CRPD and the Refugee Commission.

Fire Extinguishers

During its IT audit review, the NAO was pleased to learn that all the 10 Entities falling within the scope of this evaluation were equipped with fire extinguishers.

To this extent, the NAO observed that seven of these Entities, namely, Malita Investments p.l.c., the MCAST, the Malta Enterprise Corporation, the Malta Freeport Corporation Ltd., the Manoel Theatre, the REWS and WasteServ Malta Ltd., were equipped with fire extinguishers in strategic positions throughout the Entity's building/s or premises.

With regards to the remaining Entities, the Refugee Commission had four fire extinguishers on each of its two floors at its premises, whilst the MCCAA had at least one fire extinguisher placed on each floor of its building. Furthermore, the CRPD's main offices were also equipped with fire extinguishers, with the exception of the Entity's board room and its resource centre.

Whilst assessing the availability and placement of such fire extinguishers, the NAO also sought to ascertain that these devices were being inspected and serviced on a regular basis, by professionally and suitably equipped companies.

In this regard, the audit team observed that the fire extinguishers were being inspected and serviced regularly. During its audit visits, the NAO noted that all Entities' fire extinguishers had been inspected at least once in the prior year, with the earliest inspection carried out in March 2015 at the Manoel Theatre, and the latest in February 2016 at the MCAST. NAO also noted that WasteServ Malta Ltd. had just installed new fire extinguishers at some of its premises, and these were yet to be inspected and serviced for the first time.

All the Entities' fire extinguishers were scheduled for the next inspection at the end of a year period from the last recorded service date.

6.3 Server and Network Monitoring

The IT audit also reviewed the server and network monitoring tools used by the Entities.

Monitoring Tools for Servers and Network Equipment

This Office was informed that four of the 10 Entities under review in fact have such tools enabling them to monitor servers and network equipment. These four Entities include WasteServ Malta Ltd., the Malta Enterprise Corporation, the MCAST and the REWS.

WasteServ Malta Ltd. explained that it is equipped with Simple Network Management Protocol (SNMP) sensors and ping sensors. These are used to monitor server and network equipment along with a Paessler Router Traffic Grapher (PRTG) program, which is set up so as to send an SMS in case of any critical services being down, or an e-mail in case of default by low priority equipment.

The Malta Enterprise Corporation claimed that the servers and network equipment are monitored by free software monitoring tools, as well as other software applications and utilities supplied by the respective hardware manufacturers. To this extent, a specific proprietary software monitors the network equipment, whilst a web application, is used to monitor servers. Notwithstanding, the Entity disclosed its intentions to integrate these applications with a new system that it is planning to introduce.

The MCAST disclosed that it mostly uses a specific virtual machine software to monitor its server, whilst its network and Internet connectivity are protected and monitored using the firewall's graphical user interface.

On the other hand, the REWS only commented that it is using standard in-built tools, such as event and performance viewers found in the Microsoft Windows operating system, to monitor its systems.

The NAO also observed that Malita Investments p.l.c., the MCCAA, the Manoel Theatre, and the CRPD all confirmed that they have no such server and network monitoring tools.

Meanwhile, the Malta Freeport Corporation Ltd. and the Refugee Commission both claimed that such monitoring is only carried out by MITA.

Uninterrupted Power Supplies

The NAO also sought to verify whether any uninterrupted power supplies (UPS) are connected to the server/s, in order to counteract any unexpected power failures or power surges, and whether these are being monitored and tested on a regular basis by suitably qualified individuals/3rd party suppliers.

In this regard, the NAO observed that seven of the Entities under review stated that their servers are connected to at least one UPS. The exceptions to this approach were Malita Investments p.l.c., the MCCAA, and the CRPD, although, the MCCAA further claimed that an exercise is underway in order to have these devices installed and connected to its server/s.

The NAO also noted that those entities having a UPS/s installed and connected to their server/s, adopt different testing techniques.

In fact, the Malta Freeport Corporation Ltd., the Manoel Theatre, and the Refugee Commission have such devices installed and connected to their servers, although, these UPSs are not being monitored or tested.

Similarly, WasteServ Malta Ltd. has its equipment backed up by a UPS, and its servers connected to two different UPSs. Nonetheless, this Entity did not indicate whether these devices are being monitored and tested or not, but it was stated that batteries are changed annually by the Entity's IT unit.

In contrast, the Malta Enterprise Corporation, which also has UPS/s connected to its server/s, stated that these are monitored and tested internally, whilst adding that it is planning to phase out the current monitoring software application, and replace it with a different system.

Meanwhile, MCAST claimed that its UPSs are being monitored through a web interface, although it failed to indicate the type or name of the software used, and who monitors and tests these UPSs. However, it added that UPS batteries are replaced at least every four or five years.

Likewise, the REWS also claimed to have batteries on its UPS replaced on a regular basis, whilst adding that its UPS is monitored and occasionally tested by internal IT staff.

Conclusions and Recommendations

Upon reflecting on the above observations, the NAO is of the opinion that each of the Entities should invest in a suitable, robust and reliable monitoring system or application for its servers and network equipment. To this extent, a well tested, proven and supported software application should be used. Such software application should ideally be configured to send automatic notifications in case of any default. This Office considers this especially relevant, when taking into consideration that these systems are the backbone and hub of all the electronic communication, within these Entities. Finally, servers should always be connected to and safeguarded by a UPS.

6.4 Adequacy of Server Room

During the course of this IT audit, the NAO also held site inspections at the Entities Server Rooms. The NAO notes that four out of the 10 audited entities did not have a server room. These included the Malta Freeport Corporation Ltd. who did not have a server on-site and hosted all its data at MITA. However the other three Entities had their servers located in their offices and not in a segregated purposely refurbished server room.

Furthermore, the NAO noted that some server rooms were being also used as document repositories, workshops or stores for obsolete hardware. The NAO deems this practice to be a safety and security hazard.

Temperature and Humidity Controls at the Server Rooms

With reference to the physical environment within the Entities' server rooms, the IT audit also sought to assess how each Entity monitors and is alerted to any fluctuations in ambient temperature and humidity within these server rooms.

In this regard, the Malta Enterprise Corporation has a monitoring system with preset temperature and humidity values installed in its server room. Similarly, MCAST's server room is equipped with sensors connected to a temperature monitoring device that is accessible through a secure web interface. Additionally, both these Entities claimed that their systems feature an automatic e-mail notification/ alert mechanism, that will be triggered in the event that the predefined ambient temperatures thresholds are exceeded.

Furthermore, WasteServ Malta Ltd. has a stand-alone temperature and humidity indicator on site in its server room, however, it has no remote access or automatic notification/alert system to detect any fluctuations in temperature or humidity.

Likewise, the Manoel Theatre also claimed to have temperature and humidity controls present in its server room. Nevertheless, the Entity did not submit any further information on these devices/ mechanisms, but remarked that the Entity's security personnel monitor temperature and humidity parameters on a daily basis. Upon inspection of the Manoel Theatre's server room, the NAO did not see such controls and given the physical location of this room, the NAO believes that controlling temperature and humidity levels is very difficult without taking other physical measures such as changing the room's apertures.

Meanwhile, the MCCAA only commented that temperature inside the Entity's server room is kept constant using an air-conditioning system. During an audit visit, the NAO noted that MCCAA does not have any monitoring applications or notification/alert systems installed in its server room.

In contrast, the REWS admitted that they do not have any temperature or humidity monitoring controls in place at their server room.

Fire Suppression at the Server Room

The NAO also made enquires on the type of fire suppression systems being used at the Entities' server room.

The NAO noted that DuPont's FM-200 (also known as HFC-227ea) was the fire suppression agent selected for the server rooms and the media storage sites at the MCAST, the REWS and WasteServ Malta Ltd. It also transpired that the MCCAA has selected Carbon Dioxide (CO^2) for use within its server room and media storage site.

To this extent, the NAO was disappointed to learn that both the Malta Enterprise Corporation and the Manoel Theatre, reported that they have no fire suppression system at all in their server room.

Conclusions and Recommendations

The NAO strongly recommends that all Entities' place their servers in a purposely refurbished server room and ensure that such rooms are:

- Solely dedicated to hosting the server/s, are not used as workshops or as repository for obsolete hardware or physical files.

- Kept clean and free from clutter.

- Free from curtains, carpets and other fire hazards.

- Kept under lock and key and a log of who accessed the room with the date and time, in maintained (vide 7.2 Unauthorised Physical Access).

- Equipped with temperature and humidity controls and have monitoring tools in place, including automatic e-mail notifications in the event of substantial fluctuations.

- Equipped with a distribution surge protector.

- Equipped with two air-conditioning units which are kept on at all times and maintained regularly.

- Equipped with an adequate fire suppression system.

The NAO suggests that should having a purposely refurbished server room not be possible, the Entity concerned should discuss with its Ministry CIO so as to examine the possibility and feasibility of server re-location to a secure server room.

Chapter 7

Access Control

Chapter 7

Access Control

Access Control is a security measure that can be used to restrict, monitor, control and protect the use of an Entity's resources in a computing environment. This is achieved by regulating access or partial access to a resource or data.

There are two main types of access control: logical and physical. Whilst logical access limits connections to computer networks, system files and data; physical access controls limit access to buildings, particular rooms and/or physical IT assets.

7.1 User Authentication and Password Management

User authentication is the process by which a user proves his identity to a system, normally by logging in using a uniquely identifiable username, which is assigned to a named individual, and a password.

Therefore passwords are a primary means to control access to systems and provide the first line of defence against improper access and compromise of sensitive information.

During the IT audit, the NAO noted that although all the audited Entities implemented a login and password mechanism to log on to their PC's and to access the Entity's software applications, not all the Entities are following the password security best practices, in terms of password strength, the re-use of passwords, password expiry and failed logon attempts. The NAO also noted that whilst MITA has adopted a standard naming convention for user accounts, such naming convention is not being followed for user accounts that are not being managed by MITA.

The NAO further noted that:

- Malita Investments p.l.c. did not implement any password complexity rules neither on their PCs nor on the software applications used. Furthermore, passwords do not expire and failed logon attempts are not resulting in a locked account. Meanwhile, administrative passwords are kept in a secured envelope under lock and key.

- The MCCAA, MCAST, the Manoel Theatre and the Malta Freeport Corporation Ltd., REWS only implemented a password complexity rule when users log on to their PC's and when accessing e-mail. Some of the software applications used in the above mentioned audited entities lacked the necessary controls to ensure the mandatory use of complex, non re-usable passwords and to limit the number of failed logon attempts. In the case of Manoel Theatre there are two sets of administrator passwords, one used by the IT service provider whilst the other one given to the CEO.

- The Malta Enterprise Corporation has implemented password complexity rules on both its PC's and its software applications. Moreover, passwords expire after a defined number of days and can only be re-used after three successful password changes. Invalid login attempts are tracked and three failed attempts will result in a temporary account lockout. A hard copy of all administrative passwords is stored in a fire proof safe.

- The Commission for the Rights of Persons with Disability and the Refugee Commission have implemented password complexity rules on both their PC's and software applications. All passwords are set to expire and cannot be re-used in the immediate term. Invalid login attempts are however not being tracked. The Commission for the Rights of Persons with Disability keeps a hard copy of its administrator passwords in a secure place.

- WasteServ Malta Ltd. has implemented password complexity rules on both its PC's and software application. Passwords are set to expire after a defined number of days and cannot be re-used within a stipulated timeframe. Furthermore, invalid logon attempts are being tracked and the account is temporary locked after a defined number of unsuccessful attempts. Finally, administration passwords are changed on a yearly basis and are known by two persons only namely, the IT Officer and the IT Administrator.

The NAO also examined the procedures in place to re-issue a new password in the case of forgotten passwords and the procedures used to disable or terminate access for employees on prolonged leave, such as a career break or employees who be terminating their job. The NAO noted that:

- Malita Investments p.l.c. has no procedures in place and never encountered any issues in this regard

- Users at the MCCAA, the Malta Freeport Corporation Ltd. and the Refugee Commission contact MITA's Service Call Centre whenever a new password is required. MITA's service call centre will then raise an incident request on the user's behalf and provide a temporary password to the person in-charge, which must be then changed upon first logon. An electronic request for service (eRFS) form is submitted to MITA by the Head of IT, whenever a user account needs to be deleted upon termination of employment. Meanwhile employees on prolonged leave do not have their access suspended. However MITA automatically disable accounts if these are not used for three months. In this regard, the NAO was informed that the Refugee Commission performs yearly audits to verify the list of active users.

- The Malta Enterprise Corporation gives the user the option to call at the IT section and request a change in his/her password through a password interface. Alternatively, a user's password can be changed by the IT personnel and once the new password is communicated to the user, he/she change this password upon first logon. Whenever an employee terminates his/her employment, the Human Resources (HR) department informs the IT section accordingly and access is disabled. Moreover, the IT section periodically cross-checks the list of domain user accounts with another list supplied through the Entity's payroll package so as to ensure that user accounts which are no longer in use are disabled accordingly. On the other hand, user accounts of employees which are inactive for a pre-set number of days are flagged using an automated procedure that disables all inactive accounts. The NAO was informed that in most cases, such employees would still need to access their e-mail.

- Users at Manoel Theatre contact the supplier directly if they need their password to be reset. It is however unclear whether the users are obliged to change their given password upon first logon. The supplier is also informed accordingly when user access needs to be disabled. Employees on prolonged leave do not have their access suspended.

- Users at WasteServ Malta Ltd. need to contact the IT section whenever they need to reset passwords. It is however unclear whether the users are forced to change their given password upon first logon. The user accounts of employees who have terminated their employment are disabled by the IT section upon notification from the HR department. WasteServ Malta Ltd. has no policy in place, regarding access to employees on prolonged leave. However, this Entity only encountered one case of a person on prolonged career break in the past eight years, and in this instance access was disabled.

Conclusions and Recommendations

The NAO recommends that:

- All Entities review their user accounts and ensure that the username follows the standard naming convention implemented by MITA. Assistance from the Ministry's CIO office should be sought in this regard.

- All user accounts should adhere to the GMICT password policy[19] in terms of password complexity, password expiry, password history and the need to force the user to change the password upon first logon. Government Entities should thus implement the minimum password length policy that prohibits the use of blank passwords and ensure that passwords are set to a minimum of eight characters in length. All passwords must meet the complexity requirements policy setting, which defines that new passwords meet basic strong password requirements, with a mix of letters, numbers and symbols. Government Entities should also ensure that user account passwords are set to expire over a specified number of days.

[19] https://mita.gov.mt/en/GMICT/Pages/Security.aspx

- All Entities should carry out periodic checks to identify inactive domain user accounts and take action accordingly. This recommendation particularly applies to Entities whereby action is only taken if the IT section is notified by other internal departments about employees who no longer require access due to termination of employment.

- Once it has been established that a domain account is no longer needed, the same procedure should apply to all the user accounts used to access software applications.

- The Management of all Government Entities should review software access authorisation of users on prolonged leave. This may involve disabling access to a particular account temporarily. The above does not apply for access to e-mail services.

- Hard copies listing all administrator passwords are to be kept in a separate, clearly-labelled, sealed and signed envelopes, which must then be stored securely under lock and key. In the event that access is needed, to any one of these passwords, a register is to be kept so as to log the person accessing such password, the date, time and reason and such password is to be changed and the new password should then be kept in a sealed envelope replacing the old one. This must be done to ensure that the old admin password was not written down or saved locally on the PC/server.

- The NAO also recommends that Government Entities issue communications from time to time to remind their employees about the importance of passwords and lessen the security threats emanating from human factors, such as the sharing of passwords.

7.2 Unauthorised Physical Access

During the audit, the NAO examined the physical access to the server rooms at the 10 audited Entities and noted that:

- Malita Investments p.l.c., the Commission for the Rights of Persons with Disability, the Refugee Commission and the Malta Freeport Corporation, have no server room.

- Server rooms at the MCAST, the MCCAA, the REWS and the Manoel Theatre are kept under lock and key. Furthermore, Manoel Theatre keeps a log book recording access to the server room.

- The server room at the Malta Enterprise Corporation has been fitted with electronic door locks and a biometric reader.

- The server room at WasteServ Malta Ltd. has been fitted with electronic door locks and a swipe card reader.

Conclusions and Recommendations

The NAO noted that a particular server room was fitted with a wooden door that albeit locked could be easily opened using little force. This same server room also had access to an internal courtyard through another similar wooden door and was prone to flooding or pest infestation. The NAO recommends that the Ministry CIOs inspect the server rooms at the Government Entities that fall under their Ministry Portfolio to ensure the adequacy of such rooms and help Government Entities rectify such situations as soon as possible.

The NAO recommends that Entities keep a log book to record the details of who accessed their server rooms recording the date/time and the reason why this room was accessed. Furthermore, third party service providers should never be left unaccompanied in server rooms.

Chapter 8

Management Comments

Chapter 8

Management Comments

The following comments were submitted by each of the 10 Entities audited by way of management comments.

8.1 Malita Investments p.l.c.

The following comments were submitted by the Malita Investments p.l.c. by way of Management Comments.

The management would firstly like to thank the NAO for their recommendations, which will definitely be taken on board. As mentioned in the Company structure, what needs to be taken into consideration is that the Company employs three people and therefore although we understand that some recommendations make sense for larger organisations, they do not apply in our context.

Most of the recommendations posed by the NAO will be implemented once the Company moves to its new premises which is expected in Q2, 2017. The Company will ensure that it will have a network diagram depicting its LAN setup. We will also look into having an audit trail mechanism on our data server, however we still need to get a consultation on this. The Company will be drafting an internet and e-mail usage policy as recommended, during the course of this year.

Backups are run daily outside office hours to prevent disruption. Since the backup is hosted in our premises, in order to ensure that there is no loss of data, a second backup will be done elsewhere. With respect to smoke detectors, this needs to be looked into together with the owners of our leased offices. Moreover, it will also be ensured that in the new offices, our server will be placed in a secured server room.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services								
	Website			▨					
	Use of social media	Not Applicable							
	Servers and Data Storage Hardware								
	Local Area Network (LAN)			▨					
Chapter 2	Audit Trails								
	Information Classification Policy								
	Data Retention and Storage Policy								
	Hardware Disposal								
Chapter 3	Training Programme	Not Applicable							
	User Manuals	Not Applicable							
	Internet and E-mail usage policy			▨					
	Web Filtering Policy								
	User Awareness of Cyber Risks	Not Applicable							
Chapter 4	Anti-Virus Software								
	Patch Management				▨				
	Use of Portable Smart Media and Storage Devices								
Chapter 5	Business Continuity and Disaster Recovery Plans								
	Backup								
	Storage of Backup Media								
	Recovery of Data			▨					
Chapter 6	IT Inventories	Not Applicable							
	Physical Security								
	Server and Network Monitoring								
	Adequacy of Server Room			▨					
Chapter 7	User Authentication and Password Management			▨					
	Unauthorised Physical Access								

Table 4: Implementation Schedule - Malita Investments p.l.c.

8.2 Malta College of Arts, Science and Technology

The following comments were submitted by the Malta College of Arts, Science and Technology by way of Management Comments.

MCAST is very pleased to note that your office recognised our continuous effort and declared, MCAST to be one of the most prepared against Cyber Security Threats. This will encourage us to increase our effort and energy to maintain such alertness.

MCAST's comments on recommendations

1.4.2 Website

MCAST shall look into the compliance of its Website to the Government Website Policy and where feasible will amend accordingly.

1.4.3 Use of Social Media

It is MCAST's vision to allow the Institutes and Main Departments to have their own Facebook Page whilst retaining one corporate image. During the past year, action was taken to get all Institutes to ensure that their Facebook pages look and feel the same to the MCASTs main Facebook Page. MCAST is also enforcing the requirement that any Institute having its own Social Media presence is to nominate an individual to act as the administrator for that presence.

1.4.4 Servers and Data Storage Hardware

MCAST does not currently store Personal or Sensitive data on the Cloud.

2.1 Audit Trails

MCAST has already during the past year enabled the Audit Trails in the Dakar Software. With reference to the Access Dimensions, although an Audit Trail in the traditional sense is not there, each transaction has details attached to it with data normally found in an Audit Trail. MCAST feels that until such software is replaced, the present functionality is sufficient for our needs. Any new purchase for software will include a specific requirement for Audit Trails to be included.

2.2 Information Classification Policy

MCAST agrees that such a policy would be beneficial and will embark on a process to create and implement one.

2.3 Data Retention and Storage Policy

MCAST has already started establishing such retention periods for the various types of documents. MCAST will also create and implement a Document Retention Policy in the coming months.

A procedure to establish the proper way to dispose of any expired documents, will also be created as an appendix to the Document Retention Policy, mentioned earlier. Co-ordination and advice will be sought for this from the Office of the National Archivist.

MCAST already follows the guidelines in the Government HR Retention Policy for its HR Documents.

3.1 Training Programme

During the past year, MCAST has been re-organising its HR Department and its operations. Progress has been made with regards to orientation and training of new employees. Refresher courses for MCAST's existing staff will be organised in the future, in fact MCAST employed the services of an HR Manager specifically to plan, organise and manage such activities.

3.3 lnternet and Email Usage Policy

MCAST's lT Department feels that the best way to issue periodic reminders to MCAST's staff (and students), rather than through an email is by publishing a digital and regular Newsletter. Such a Newsletter has already been designed and a prototype created. lt is planned that such a Newsletter will start being sent to MCASTs staff and students in the near future.

3.5 User Awareness of Cyber Risks

See comment for 3.3 above, same applies here.

4.2 Patch Management

During the past months, MCAST established a centralised server (WSUS Server), through which all updates, fixes and patches are managed and deployed.

4.3 Use of Portable Smart Media and Storage Devices

MCAST will be updating its Wi-fi Policy to reflect the recommendation made by the Report. See also comments for 3.3 above as the same applies here too.

5.1 Business Continuity and Disaster Recovery Plan

MCAST agrees with the recommendations made by the NAO and will embark on the creation of a Business Recovery Plan and a Disaster Recovery Plan to reflect the actual procedures in use at MCAST with regards to these two requirements.

6.1 IT Inventories

MCAST has just finalised an internal audit with regards to Software Licences currently in use across all over MCAST. MCAST is now in the process of setting up an Inventory of such Software Licences.

6.2 Physical Security

MCAST will be drafting a Visitors' Policy to complement and codify the procedure already in place.

6.3 Server and Network Monitoring (Uninterrupted Power Supply)

The IT staff under the supervision of the IT Manager make use of the APC proprietary software to monitor the UPS in use at MCAST's Server Room. The IT Manager also oversees regular testing of the said UPS in use.

7.1 User Authentication and Password Management

MCAST feels that its current procedure in place is adequate and sufficient especially when one considers the number of people (staff and students) making daily and regular use of the system.

MCAST would like to implement a Digitised Access Control to the Server Room, which would automatically control and log access to it.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services	Not Applicable							
	Website			▨					
	Use of social media	Not Applicable							
	Servers and Data Storage Hardware	Not Applicable							
	Local Area Network (LAN)	Not Applicable							
Chapter 2	Audit Trails	Not Applicable							
	Information Classification Policy			▨					
	Data Retention and Storage Policy			▨					
	Hardware Disposal	Not Applicable							
Chapter 3	Training Programme		▨		▨				
	User Manuals	Not Applicable							
	Internet and E-mail usage policy		▨						
	Web Filtering Policy	Not Applicable							
	User Awareness of Cyber Risks				▨				
Chapter 4	Anti-Virus Software	Not Applicable							
	Patch Management	Not Applicable							
	Use of Portable Smart Media and Storage Devices		▨						
Chapter 5	Business Continuity and Disaster Recovery Plans			▨					
	Backup	Not Applicable							
	Storage of Backup Media	Not Applicable							
	Recovery of Data	Not Applicable							
Chapter 6	IT Inventories	▨							
	Physical Security			▨					
	Server and Network Monitoring	Not Applicable							
	Adequacy of Server Room	Not Applicable							
Chapter 7	User Authentication and Password Management	Not Applicable							
	Unauthorised Physical Access				▨				

Table 5: Implementation Schedule - MCAST

8.3 Malta Competition and Consumer Affairs Authority

The following comments were submitted by the Malta Competition and Consumer Affairs Authority by way of Management Comments.

MCCAA noted with satisfaction the audit report produced by the NAO as this will give us guide on different aspects such as security, procedures and policies.

This year, MCCAA will be embarking on a process of creating new IT policies, which will establish different procedures mentioned in the report such as backup procedures, use of portable smart media, Internet and e-mail usage policy, offline email backup, data retention and storage policies. A primary benefit to MCCAA is to help staff to initiate actions and take responsibility without constant reference to management.

This year, MCCAA is committed to create a Disaster Recovery Plan and a Business Continuity Plan, which will be in-line with MCCAA's mission, strategic goals and objectives. The documentation will provide the MCCAA management with an understanding on the adverse effects in case of service disruption and the total effort required to develop and maintain an effective BCP.

MCCAA is already in talks with MSDC IMU to improve the current IT hardware disposal procedure and the integration a software inventory to current asset management. MCCAA is currently in the process of upgrading indicated asset to Microsoft Office 2016.

Currently works are in progress to bring the MCCAA server room up to required standards, such as UPS installations to all network equipment, network diagrams, and network monitoring utilities. Implementation of servers audit trails and password complexity is in place after the first audit visit.

MCCAA will ask MITA for periodic reports on anti-virus updates. This will allow verification of update antivirus on the current assets MCCAA have. The Authority is in the process of transferring local servers onto MITA virtual environment, which will allow the backup process to be easier and more efficient. In the meantime, a study done on current backup of local server showed that recovery procedure is effective.

MCCAA is currently in the process of redesigning a new system, thus will integrate manuals accordingly. The availability of manuals will allow easy training of the new system to employees and new recruits. This new system will allow users to authenticate with passwords that are more complex. A new MCCAA Portal is included in the new system, which will be according to government policies.

MCCAA is in the process of removing old Facebook page that could mislead the public. To avoid this, MCCAA have embarked in different promotion material to promote the company and its Facebook official page to the public.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services	Not Applicable							
	Website					▨			
	Use of social media				▨				
	Servers and Data Storage Hardware	Not Applicable							
	Local Area Network (LAN)				▨				
Chapter 2	Audit Trails			▨					
	Information Classification Policy				▨				
	Data Retention and Storage Policy				▨				
	Hardware Disposal			▨					
Chapter 3	Training Programme					▨			
	User Manuals					▨			
	Internet and E-mail usage policy				▨				
	Web Filtering Policy	Not Applicable							
	User Awareness of Cyber Risks	Not Applicable							
Chapter 4	Anti-Virus Software				▨				
	Patch Management	Not Applicable							
	Use of Portable Smart Media and Storage Devices				▨				
Chapter 5	Business Continuity and Disaster Recovery Plans	Not Applicable							
	Backup				▨				
	Storage of Backup Media				▨				
	Recovery of Data				▨				
Chapter 6	IT Inventories				▨				
	Physical Security	Not Applicable							
	Server and Network Monitoring	Not Applicable							
	Adequacy of Server Room					▨			
Chapter 7	User Authentication and Password Management					▨			
	Unauthorised Physical Access	Not Applicable							

Table 6: Implementation Schedule - MCCAA

8.4 Malta Enterprise Corporation

The following comments were submitted by the Malta Enterprise Corporation by way of Management Comments.

Malta Enterprise welcomes all comments and recommendations presented in this report and proposes the following actions in order to address its shortages as per below:

Website – In consultation with our Internal Audit we shall be conducting an audit of our website to ensure that it complies with the suggested Government Website Policy.

Data retention and storage policy – An updated policy has already been drafted which, upon approval from the management, would be published in our intranet site to be made available to all employees.

Training Programme – Malta Enterprise concurs with the NAO in that, although we do provide an overall induction process and on-the-job IT training to all employees there is still the need to formalize an induction program to all new recruits that is specific to IT.

User awareness of cyber risks – Currently we are in discussion with the Institute for Public Service to provide our users with the recommended "Information Security Awareness" course. This will be delivered in our own premises with classes of up to 10 students.

Business continuity and disaster recovery plans – Although we do have plans on how we can operate in case of a total failure, such plans would be formalized and documented.

Visitor's Policy – Our manual procedure is bound to be replaced with an electronic guestbook. Also, we shall be including a new Visitor's Policy in consultation with our Internal Audit.

Fire suppression at the server room – We shall be contacting our Fire Engineer to provide an evaluation of the area and recommend us with a way forward on adequate measures to be taken.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services	Not Applicable							
	Website		▨						
	Use of social media	Not Applicable							
	Servers and Data Storage Hardware	Not Applicable							
	Local Area Network (LAN)	Not Applicable							
Chapter 2	Audit Trails	Not Applicable							
	Information Classification Policy	Not Applicable							
	Data Retention and Storage Policy		▨						
	Hardware Disposal	Not Applicable							
Chapter 3	Training Programme		▨						
	User Manuals	Not Applicable							
	Internet and E-mail usage policy	Not Applicable							
	Web Filtering Policy	Not Applicable							
	User Awareness of Cyber Risks			▨					
Chapter 4	Anti-Virus Software	Not Applicable							
	Patch Management	Not Applicable							
	Use of Portable Smart Media and Storage Devices	Not Applicable							
Chapter 5	Business Continuity and Disaster Recovery Plans			▨					
	Backup	Not Applicable							
	Storage of Backup Media	Not Applicable							
	Recovery of Data	Not Applicable							
Chapter 6	IT Inventories	Not Applicable							
	Physical Security		▨						
	Server and Network Monitoring	Not Applicable							
	Adequacy of Server Room		▨			▨			
Chapter 7	User Authentication and Password Management	Not Applicable							
	Unauthorised Physical Access	Not Applicable							

Table 7: Implementation Schedule - Malta Enterprise Corporation

8.5 Malta Freeport Corporation Ltd.

The following comments were submitted by the Malta Freeport Corporation Ltd. by way of Management Comments.

The management of Malta Freeport Corporation Ltd. were pleased to assist in the IT Audit Report prepared by the National Audit Office and welcomes their recommendations which will be implemented according to the presented schedule.

Currently all IT requirements at Malta Freeport Corporation Ltd. are out-sourced to MITA, however, a specific person will be appointed to oversee all IT requirements. The website will eventually need upgrading but this will be done at a later stage. The Local Area Network diagram has been submitted.

We plan to put the necessary policies/procedures in respect of data management and governance in place by early next year with the assistance of the CIO from the Ministry's Information Management Unit.

Most of our training is done in-house on the job, however, we will endeavour to have a formal documented training strategy in place. We will also ensure that our employees attend the 'Information Security Awareness' course organised by the Institute for Public Services by the end of the year. We will implement a procedure to make sure that offline mailboxes are being backed up internally.

Anti-virus software and patch management are provided by MITA through our IT outsourcing contract, however, we will be asking MITA to produce periodic reports. We plan to implement policies, procedures and software requirements for the use of portable smart media and storage devices by the 2nd quarter of 2018.

We do not currently have a business continuity plan BCP or a disaster recovery plan DRP in place and will be working on developing a BCP and DRP designed to ensure continuity of the day to day running of our business. MITA is contracted to take our backup periodically. We will be contacting MITA to establish a schedule for restores.

We will be updating our software inventories as recommended. We are fully compliant with physical security and user/password authentication.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services	▨							
	Website								▨
	Use of social media	Not Applicable							
	Servers and Data Storage Hardware	Not Applicable							
	Local Area Network (LAN)	Not Applicable							
Chapter 2	Audit Trails					▨			
	Information Classification Policy					▨			
	Data Retention and Storage Policy					▨			
	Hardware Disposal		▨						
Chapter 3	Training Programme				▨				
	User Manuals	Not Applicable							
	Internet and E-mail usage policy		▨						
	Web Filtering Policy	Not Applicable							
	User Awareness of Cyber Risks				▨				
Chapter 4	Anti-Virus Software		▨						
	Patch Management	Not Applicable							
	Use of Portable Smart Media and Storage Devices						▨		
Chapter 5	Business Continuity and Disaster Recovery Plans								▨
	Backup	Not Applicable							
	Storage of Backup Media	Not Applicable							
	Recovery of Data		▨						
Chapter 6	IT Inventories		▨						
	Physical Security	Not Applicable							
	Server and Network Monitoring	Not Applicable							
	Adequacy of Server Room	Not Applicable							
Chapter 7	User Authentication and Password Management	Not Applicable							
	Unauthorised Physical Access	Not Applicable							

Table 8: Implementation Schedule - Malta Freeport Corporation Ltd.

8.6 Manoel Theatre

The following comments were submitted by the Manoel Theatre by way of Management Comments.

Referring to the recommendations listed in the IT Audit Report, Teatru Manoel will be adopting all the recommendations suggested by the NAO. These will be implemented by the end of this year.

During 2017 Teatru Manoel will be issuing a call for applications to recruit an IT person to be responsible of the Teatru Manoel IT requirements. In addition to this Manoel Theatre will be approaching the Office of the CIO, within the Ministry of Justice, Culture and Local Government in order to review the IT Operations as suggested by NAO.

Teatru Manoel have recently contacted MITA and an upcoming meeting will be held to explore the possibility to migrate the Teatru Manoel IT within the MITA prescribed parameters.

With regards the ticketing system of Teatru Manoel, within the next few months our booking system will be migrating to the central ticketing system of the Arts Council Malta.

The Visitors Policy is in the process to be part of the project which will be discussed with MITA.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services				▨				
	Website				▨				
	Use of social media	Not Applicable							
	Servers and Data Storage Hardware				▨				
	Local Area Network (LAN)				▨				
Chapter 2	Audit Trails				▨				
	Information Classification Policy				▨				
	Data Retention and Storage Policy				▨				
	Hardware Disposal				▨				
Chapter 3	Training Programme				▨				
	User Manuals				▨				
	Internet and E-mail usage policy				▨				
	Web Filtering Policy				▨				
	User Awareness of Cyber Risks				▨				
Chapter 4	Anti-Virus Software				▨				
	Patch Management				▨				
	Use of Portable Smart Media and Storage Devices				▨				
Chapter 5	Business Continuity and Disaster Recovery Plans				▨				
	Backup				▨				
	Storage of Backup Media				▨				
	Recovery of Data				▨				
Chapter 6	IT Inventories				▨				
	Physical Security				▨				
	Server and Network Monitoring				▨				
	Adequacy of Server Room				▨				
Chapter 7	User Authentication and Password Management				▨				
	Unauthorised Physical Access				▨				

Table 9: Implementation Schedule - Manoel Theatre

8.7 Commission for the Rights of Persons with Disability

The following comments were submitted by the Commission for the Rights of Persons with Disability by way of Management Comments.

CRPD will do its utmost to adhere with the recommendations given in this report. We found this exercise very useful since we were not aware of most of the points highlighted and look forward to implementing what is required from our entity.

In view of the fact that CRPD will be moving into new premises (currently in shell form) later on this year, following recommendation given by the NAO, we have started discussions with MFSS' CIO and the contractor to assure that basic IT needs (network points, ideal place for server room, quality of cables, etc) are targeted from the very beginning.

With regards to other recommendations, we fully understand the need to work on a plan (with short, medium and long term time-frames) which would eventually put CRPD in compliance with this report.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services							▨	
	Website				▨				
	Use of social media	Not Applicable							
	Servers and Data Storage Hardware	Not Applicable							
	Local Area Network (LAN)					▨			
Chapter 2	Audit Trails					▨			
	Information Classification Policy						▨		
	Data Retention and Storage Policy					▨			
	Hardware Disposal		▨						
Chapter 3	Training Programme						▨		
	User Manuals						▨		
	Internet and E-mail usage policy			▨					
	Web Filtering Policy				▨				
	User Awareness of Cyber Risks			▨					
Chapter 4	Anti-Virus Software		▨						
	Patch Management						▨		
	Use of Portable Smart Media and Storage Devices					▨			
Chapter 5	Business Continuity and Disaster Recovery Plans						▨		
	Backup					▨			
	Storage of Backup Media		▨						
	Recovery of Data		▨						
Chapter 6	IT Inventories					▨			
	Physical Security					▨			
	Server and Network Monitoring					▨			
	Adequacy of Server Room				▨				
Chapter 7	User Authentication and Password Management						▨		
	Unauthorised Physical Access					▨			

Table 10: Implementation Schedule - CRPD

8.8 Refugee Commission

The following comments were submitted by the Refugee Commission by way of Management Comments.

The Office of the Refugee Commissioner is pleased to note that the NAO recognised the efforts made by the former office in order to improve the situation with respect to IT and appreciates the recommendations made. The Office of the Refugee Commissioner will also strive to implement many of the recommendations made as can be seen from the Recommendations Implementations Schedule. It should also be noted that certain recommendations made in the schedule, namely, the Use of Social Media, the Web Filtering Policy and the User Awareness of Cyber Risks, are not applicable to this Office due to its particular nature. Moreover, the Office of the Refugee Commissioner would also like to point out that Teleworking is carried out in line with Standard Operating Procedures in order to ensure that no risks may arise. Furthermore, the Website of the Office of the Refugee Commissioner is governed by GMICT policies.

The current Refugee Commissioner wishes to clarify that she has only occupied this post for a few months prior to the closure of this audit. The Refugee Commissioner is presently taking stock of the IT situation of the Office of the Refugee Commission and shall be addressing the recommendations made by the NAO in this audit, assuming that the required resources will be made available within an adequate timeframe.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services		▨						
	Website						▨		
	Use of social media	Not Applicable							
	Servers and Data Storage Hardware								▨ *
	Local Area Network (LAN)				▨				
Chapter 2	Audit Trails				▨				
	Information Classification Policy								▨ *
	Data Retention and Storage Policy								▨ *
	Hardware Disposal								▨
Chapter 3	Training Programme							▨	
	User Manuals								▨ *
	Internet and E-mail usage policy			▨					
	Web Filtering Policy	Not Applicable							
	User Awareness of Cyber Risks	Not Applicable							
Chapter 4	Anti-Virus Software			▨					
	Patch Management				▨				
	Use of Portable Smart Media and Storage Devices					▨			
Chapter 5	Business Continuity and Disaster Recovery Plans				▨				
	Backup								▨ *
	Storage of Backup Media								▨ *
	Recovery of Data								▨ *
Chapter 6	IT Inventories								▨ *
	Physical Security	Not Applicable							
	Server and Network Monitoring						▨ *		
	Adequacy of Server Room								▨ *
Chapter 7	User Authentication and Password Management						▨ *		
	Unauthorised Physical Access								▨ *

Table 11: Implementation Schedule - Refugee Commission

* Premises/Resources/Funding Permitting

8.9 Regulator for Energy and Water Services

The following comments were submitted by the Regulator for Energy and Water Services by way of Management Comments.

REWS management has gone through NAO's report "Cyber Security across Government Entities", and is pleased to note the generally positive feedback given in respect of its IT security.

Since the date when the fieldwork for the NAO report was carried out, an additional employee joined the IT function at REWS in the role of IT Administrator, taking the full time complement in this Unit to two employees. Another development is the introduction of cloud hosting in respect of one particular application. In making use of cloud computing, the Regulator will give due attention to the points put forward by NAO in its report.

REWS management also takes note of other NAO recommendations for improvement insofar as these are relevant to REWS and technically/financially feasible. Due consideration will be given to updating its policies as necessary, including those in respect of Information Classification, Data Retention/ Storage and Business Continuity and Disaster Recovery Plans.

The Regulator will effect improvements to its server room by adding temperature and humidity controls as recommended in the report.

Further to the above, REWS is enclosing its Recommendations Implementation Schedule setting out a timeline for addressing the matters that resulted from this report.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services	Not Applicable							
	Website								▨
	Use of social media	Not Applicable							
	Servers and Data Storage Hardware	Not Applicable							
	Local Area Network (LAN)	Not Applicable							
Chapter 2	Audit Trails	Not Applicable							
	Information Classification Policy						▨		
	Data Retention and Storage Policy						▨		
	Hardware Disposal	Not Applicable							
Chapter 3	Training Programme				▨				
	User Manuals	Not Applicable							
	Internet and E-mail usage policy						▨		
	Web Filtering Policy						▨		
	User Awareness of Cyber Risks	Not Applicable							
Chapter 4	Anti-Virus Software					▨			
	Patch Management	Not Applicable							
	Use of Portable Smart Media and Storage Devices						▨		
Chapter 5	Business Continuity and Disaster Recovery Plans						▨		
	Backup	Not Applicable							
	Storage of Backup Media	Not Applicable							
	Recovery of Data							▨	
Chapter 6	IT Inventories	Not Applicable							
	Physical Security	Not Applicable							
	Server and Network Monitoring	Not Applicable							
	Adequacy of Server Room				▨				
Chapter 7	User Authentication and Password Management							▨	
	Unauthorised Physical Access	Not Applicable							

Table 12: Implementation Schedule - REWS

8.10 WasteServ Malta Ltd

The following comments were submitted by WasteServ Malta Ltd. by way of Management Comments.

The management has reviewed the report and acknowledges the recommendations that were provided by the NAO, through the audit report on Cyber Security across Government Entities.

Management ensures that the audit recommendations will be seen and addressed to. Through-out the audit process, actions on the findings, were already being tackled to ensure that the Company is prepared for such threats.

WasteServ Audit findings have been listed below to provide an understanding on how the issues are going to be tackled:

- The un-used social media pages such as "WasteServ Tree Center" will be discussed with the PR Department and if the page is no longer required, WasteServ will backup and remove the page accordingly.
- The Company Website will be reviewed to comply with the Government Policy.
- Information Classification, Data Retention Storage Policy and Business Continuity and Disaster Recovery Plans will be discussed with CIO to draft the policies and published when completed.
- A patch management tool has already been deployed in 2017 Q1 and is being reviewed by the IT administrator prior rolling out.
- A Training Programme document shall be compiled by the IT Department together with the HR Department to provide training to WasteServ Users.
- Users are now forced to change their password after a new password is provided by the IT Department, by the use group policy.
- All WasteServ Sites are filtered according to department by the use of Web Filter, Gateway Security and Access Rules on Main Firewall.
- WasteServ had already established an Internet and e-mail Usage Policy which is located in the IT Handbook which is given to each user upon induction, first day he/she is employed. The policy will be discussed with the CIO and updated accordingly.
- Users will start receiving monthly emails on new cyber threats to have a better understanding on the type of risks when using computers.

WasteServ Management appreciates the findings that where identified by the audit report which shall enhance the Company Processes, and would like to thank the NAO auditors for their support.

Recommendations Implementation Schedule

Components		2017				2018			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 1	In-house IT Unit or Out-Sourced IT services	Not Applicable							
	Website			▨					
	Use of social media	▨							
	Servers and Data Storage Hardware	Not Applicable							
	Local Area Network (LAN)			▨					
Chapter 2	Audit Trails	Not Applicable							
	Information Classification Policy					▨			
	Data Retention and Storage Policy					▨			
	Hardware Disposal	Not Applicable							
Chapter 3	Training Programme				▨				
	User Manuals	Not Applicable							
	Internet and E-mail usage policy	Not Applicable							
	Web Filtering Policy	Not Applicable							
	User Awareness of Cyber Risks					▨			
Chapter 4	Anti-Virus Software	Not Applicable							
	Patch Management	▨							
	Use of Portable Smart Media and Storage Devices			▨					
Chapter 5	Business Continuity and Disaster Recovery Plans					▨			
	Backup	Not Applicable							
	Storage of Backup Media	Not Applicable							
	Recovery of Data	Not Applicable							
Chapter 6	IT Inventories	Not Applicable							
	Physical Security	Not Applicable							
	Server and Network Monitoring	Not Applicable							
	Adequacy of Server Room	Not Applicable							
Chapter 7	User Authentication and Password Management	Not Applicable							
	Unauthorised Physical Access	Not Applicable							

Table 13: Implementation Schedule - WasteServ Malta Ltd.

Annexes

Annex A

CoBit Controls

CoBit defines IT activities in a generic process model within four domains[20]. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate as depicted in Figure 2. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

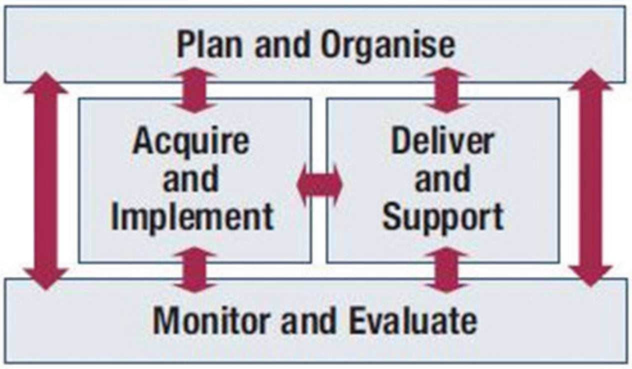


Figure 2: The Four integrated domains of CoBit

Plan and Organise

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives.

Define a Strategic IT Plan

IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and HR requirements, and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.

Assess and Manage IT Risks

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation, caused by an unplanned event, is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level.

[20] CoBit 4.1 Framework - http://www.isaca.org/Knowledge-Center/cobit/Documents/CoBit4.pdf

The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.

Acquire and Implement

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process.

Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment, are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Install and Accredit Solutions and Changes

New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed-upon expectations and outcomes.

Deliver and Support

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities.

Define and Manage Service Levels

Effective communication between IT management and business customers regarding services required is enabled by a documented definition of, and agreement on, IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels, and enables alignment between IT services and the related business requirements.

Manage Third-party Services

The need to assure that services provided by third parties, (suppliers, vendors and partners) meet business requirements requires an effective third party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third party agreements, as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third party services minimises the business risk associated with non-performing suppliers.

Ensure Continuous Service

The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilising offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.

Ensure Systems Security

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing, and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.

Manage the Physical Environment

Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.

Manage Operations

Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. An effective operation management helps maintain data integrity and reduces business delays and IT operating costs.

Monitor and Evaluate

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements.

Provide IT Governance

Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered, in accordance with enterprise strategies and objectives.

Annex B

Restrictions on use of Electronic Mail and Internet services[21]

Restrictions on use of e-mail services

Every user should abide by the restrictions on use of e-mail and should not:

- impersonate or forge the signature of any other person when using e-mail.
- amend messages received in a fraudulent manner.
- gain access to, examine, copy or delete another person's e-mail without the necessary authorisation from the person concerned.
- disclose their password or other means of access.
- use someone else's password or other means of access to a computer.
- use e-mail to harass or defame any person or group of persons.
- use e-mail to conduct any personal business or for commercial or promotional purposes.
- send as messages or attachments items that may be considered offensive, pornography, illegal material, chain letters or junk mail.
- send e-mail in bulk unless it is formally solicited.
- place Government-assigned e-mail address on non-official business cards.
- send trivial messages or copy messages to people who do not need to see them.
- send unsolicited mass e-mailing to more than twenty-five e-mail users, if such unsolicited e-mailing provokes complaints from the recipients.
- use the service of another provider, but channelling activities through a MAGNET account as a re-mailer, or use a MAGNET account as a mail drop for responses.

[21] OPM Circular No. 10/2003 - Electronic Mail and Internet Services Directive

Restrictions on use of Internet services

Similarly, every user should abide by the restrictions on the use of Internet and should not:

- download files from the Internet without adhering to existing policies on virus control.
- download material (including software) that is not work-related.
- enter into any contract over the Internet without approval from the appropriate Head of Department or his/her delegate.
- use the Internet to conduct any personal business or for personal commercial purposes.
- post a single article or advertisement to more than ten Usenet or other newsgroups, forums, e-mail mailing lists or other similar groups or lists.
- post to any Usenet or other newsgroup, forum, e-mail mailing list or other similar group or list articles, which are off-topic according to the charter or other owner-published FAQ or description of the group list.

Annex C

Business Continuity and Disaster Recovery Plan[22]

A Business Continuity Plan should:

- be documented and written in simple language and understandable to all.
- be consistent with the Entity's overall mission, strategic goals and objectives.
- provide management with an understanding on the adverse effects on the Entity, resulting from normal systems or service disruption and the total effort required to develop and maintain an effective BCP.
- assess each business process to determine its criticality.
- include a list of essential hardware, software and information assets related to core business processes.
- identify methods to maintain the confidentiality and integrity of data.
- ensure that an appropriate control environment (such as segregation of duties and control access to data and media) are in place.
- ensure that data is regularly backed up on storage media.
- ensure that appropriate backup rotation practice is in place and backups are retrievable.
- ensure that storage media are kept offsite and kept securely in a backup safe.
- identify an alternate site from which to resume operations.
- preferably include details of manual processes that could temporarily maintain operational functionality for each business process in the event of a total IT system collapse.
- include a complete DRP that amongst others lists the access rights granted following a restore.

[22] Business Continuity and Disaster Recovery Plan as per www.isaca.org

- validate the RPO and the RTO for various systems and their conformance to the Entity's objectives.

- include a plan that details how to restore operations to normality.

- identify the conditions that will activate the contingency plan.

- identify which resources would be available in a contingency stage and the order in which these will be recovered.

- identify the key persons responsible for each function in the plan.

- identify the methods of communication amongst the key persons, support staff and employees to be adopted during recovery of services.

- implement a process for periodic review of the BCP's continuing suitability as well as timely updating of the document, specifically when there are changes in technology and processes, legal or business requirements.

- develop a comprehensive BCP test approach that includes management, operational and technical testing.

- implement a process of change management and appropriate version controls to facilitate maintainability.

- identify mechanisms and decision maker(s) for changing recovery priorities resulting from additional or reduced resources as compared to the original plan.

- document formal training approaches and raise awareness across the Entity on the effect this might have on the Entity in the event of a disaster.

- be stored in hard-copy and soft-copy format both on-site and off-site.

- be distributed to members of staff, Head of Sections etc. (any confidential information should only be given to key persons on a need-to-know basis).

A DRP should form part of the BCP and shall dictate every facet of the recovery process including:

- a statement detailing the scope and capability of the DRP, exactly when this plan should be used and what the impact is on the Entity.

- a list of people in the organisation that have the authority to declare a disaster and thereby put the plan into effect.

- the sequence of events necessary to prepare the backup site once a disaster has been declared.

- an inventory of the necessary hardware and software required to restore service.

- a schedule listing the personnel that will be staffing the backup site, including, if necessary, a rotation schedule to support ongoing operations without burning out the recovery team members.

- a description of the key roles and responsibilities so that anyone assigned to a particular role in the recovery team understands what is required of him/her.

- a summary of the critical services, their recovery objectives and recovery priorities.

- third party contact details, particularly those that may be required to assist in the recovery of resources or services that are being maintained within the Entity.

- detailed recovery activities and sequence of events, including pre-requisites, dependencies and responsibilities.

Recent NAO Publications

NAO Audit Reports

February 2016	Performance Audit: Agreements between Government and Conservatorio Vincenzo Bugeja on Jeanne Antide and Fejda Homes
February 2016	Performance Audit: Service Agreements between Government and INSPIRE Foundation
April 2016	Performance Audit: An Analysis on OHSA's Operations - A Case Study on the Construction Industry
May 2016	Information Technology Audit: Mater Dei Hospital
June 2016	The General Practitioner function - The core of primary health care
July 2016	An Investigation of the 2015 Local Councils' Capital Projects Fund
July 2016	An Investigation of Local Councils Funding Schemes launched between 2008 and 2013
September 2016	Performance Audit: Service Agreements between Government and Richmond Foundation Malta
October 2016	Performance Audit: Agreements between Government and YMCA Valletta
November 2016	Performance Audit: Managing and Monitoring the State Schools' Transport Services
December 2016	Annual Audit Report of the Auditor General - Public Accounts 2015
December 2016	Annual Audit Report of the Auditor General - Local Government 2015
December 2016	An Investigation of Property Transfers between 2006 and 2016: The Transfer of Land at Ta' L-Istabal, Qormi
December 2016	An Investigation of Property Transfer between 2006 and 2013: The Acquisition of 233, 236, and 237 Republic Street, Valletta
January 2017	Contribution of the Structural Funds to the Europe 2020 Strategy in the Areas of Employment and Education

NAO Work and Activities Report

March 2016	Work and Activities of the National Audit Office 2015