Information Technology Audit

Heritage Malta

Table of Contents

List of Abbreviations

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

ADSL	Asymmetric Digital Subscriber Line
AITF	Art Information Task Force
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CCTV	Closed-Circuit Television
CDWA	Categories for Descriptions of Works of Art
CEO	Chief Executive Officer
COBIT	Control Objectives for Information and related Technology
CIMU	Central Information Management Unit
DAM	Digital Asset Management
DocReg	Document Registry
DoS	Denial of Service
DRP	Disaster Recovery Plan
DVD	Digital Versatile Disc
ESF	European Social Fund
FSS	Final Settlement Statement
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
IT	Information Technology
ITSM	Information Technology Service Management
IPS	Intrusion Prevention System
IST	Information Society Technologies
GMICT	Government of Malta Information and Communication Technology
LAN	Local Area Network
MAGNET	Malta Government Network
MCAST	Malta College of Arts, Science and Technology
Mbps	Megabits per second
MITA	Malta Information Technology Agency
NAO	National Audit Office
NAS	Network Area Storage
OA	Office Automation
OPM	Office of the Prime Minister
PC	Personal Computer
POS	Point-of-Sale
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SEP	Symantec Endpoint Protection
UNESCO	United Nations Educational, Scientific and Cultural Organisation
UPS	Uninterrupted Power Supply
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WSUS	Windows Server Update Services

Chapter 1
Introduction

Heritage Malta is the national agency for museums, conservation practice and cultural heritage. Established under the Cultural Heritage Act, which was enacted in 2002, the national agency replaced the former Museums Department.

As a public strategic partner, Heritage Malta will assume a key role in the implementation of the National Cultural Policy recently proposed by Government and Vision 2015. In this regard, the Board of Directors adopted a strategic plan intended to create agreement and give clear direction on strategic objectives, priorities and measures to be achieved. The end result will contribute towards a better appreciation of Malta's cultural heritage and the enrichment of society's quality of life.

Certain objectives covered in the strategic plan are of an ongoing nature while others will require a longer timeframe for completion. The plan focuses on the following strategic objectives:

- To manage and care for the cultural heritage for the sustainable enjoyment of present and future generations.
- To empower diverse audiences to enrich their quality of life through a positive engagement in cultural heritage.
- To foster a culture of excellence across the sector through exchange of best practices.
- To address infrastructural and restoration works in buildings and sites entrusted to the Agency.
- To manage operational functions that supports the achievement of the overall strategic objectives.

This audit report, issued by the Information Technology (IT) Audits and Operations Unit within the National Audit Office (NAO), documents the current state of IT operations within Heritage Malta. All the findings and recommendations that resulted from the risk based IT audit, are included in this report.

1.1 Background

Originally Heritage Malta was entrusted with the management of museums, sites, including seven UNESCO World Heritage sites, and their collections. As from 2005, following an amendment to the Cultural Heritage Act, all activities previously carried out by the former Malta Centre for Restoration, were taken over by Heritage Malta, which became the national agency responsible for conservation.

Heritage Malta seeks to provide its various clients with an enhanced experience during visits to the various sites and museums managed by the national agency. Cultural heritage can act as a catalyst for Malta's tourism potential and consequently contribute significantly to the economy. The agency has a specific educational section with special educational programmes targeting children of different age groups as part of organised school visits. These educational programmes are based on the educational curriculum and address specific areas of study in an edutainment way. Furthermore, the agency operates the Institute of Conservation and Management of Cultural Heritage which runs undergraduate and postgraduate academic courses in the field of conservation together with the University of Malta and vocational courses organised in conjunction with MCAST. In addition, the Institute also offers a number of short courses available to the general public.

Heritage Malta is committed to bring culture closer to the people by also providing access for persons with disabilities. Whether through temporary exhibitions, public lectures, heritage trails or other specialised events, the agency lives up to its motto *"of ensuring a future to our past"*.

Heritage Malta's subsidiary, Heritage Malta Services Limited, serves as its commercial arm for activities and events of a business nature. Its main activities include the hiring out of venues for corporate entertainment, promoting its corporate patrons programme and monitoring the museum shop activities besides other day-to-day revenue generating activities.

Chapter 1
Introduction

1.2 Organisation Structure

Heritage Malta is governed by a Board of Directors appointed by the Minister. The Board is appointed for successive three year terms. Heritage Malta is currently divided into four different units:

- ICT and Information Management unit
- Curatorial unit
- Conservation unit
- Projects unit

Apart from the above, the Visitor Services and Events Department, the Human Resources and Administration Department, the Finance Department and the Legal Affairs Department report directly to the Chief Executive Officer.

The organisation chart in Appendix A depicts how Heritage Malta is set up.

Heritage Malta Head Office is located at the ex-Royal Naval Hospital in Bighi, Kalkara and administers 24 sites and museums in Malta and seven sites and museums in Gozo. Heritage Malta also has an area office at the Cittadella in Victoria Gozo. As depicted in Figure one, Heritage Malta has a staff compliment of 257 full-time employees in Malta and 39 full-time employees in Gozo. Furthermore, four part-time lecturers are currently employed with Heritage Malta as part of the European Social Fund (ESF) 1.31 Project related to Education and Training in Wood Conservation and Restoration.

In line with Government's family friendly measures policy, there are currently 13 Heritage Malta employees working on reduced hours. To date, there are no employees working on teleworking basis. However, Heritage Malta intends to provide teleworking facilities to its employees in the near future.

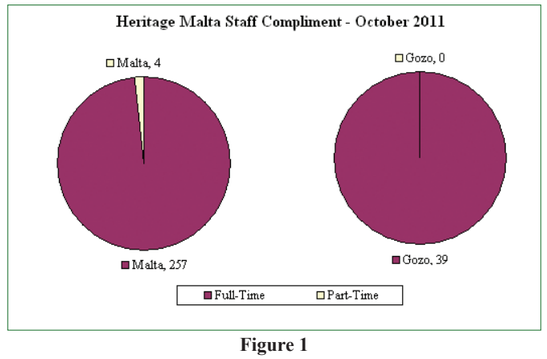


Figure 1

1.3 Legislation

Heritage Malta is regulated mainly by the following legislations:

- National Archives Act 1990, Chapter 477 of the Laws of Malta
- Freedom of Information Act, Chapter 496 of the Laws of Malta
- Environment Protection Act 2001, Chapter 435 of the Laws of Malta
- Culture Heritage Act, Chapter 445 of the Laws of Malta
- Protection of Antiquities Regulations, L.N. 445.01
- National Museums, Sites and Collections (Admission Fees) Regulations, L.N. 445.05
- Donations (National Heritage) Rules, L.N. 123.96
- National Museums and Monuments (Comprehensive Admission Tickets) Act, Chapter 298 of the Laws of Malta
- Public Curators Act, Chapter 299 of the Laws of Malta
- Periti Act, Chapter 390 of the Laws of Malta

Furthermore, Heritage Malta makes significant reference to the following legislations:

- Protection of the Maltese Language Act 2003, Chapter 470 of the Laws of Malta
- Malta Council for Culture and the Arts Act, Chapter 444 of the Law of Malta

1.4 ICT at Heritage Malta

As computer technology evolved, Heritage Malta became increasingly dependent on IT systems to carry out its operations and to process, store and maintain essential information. Taking into consideration that Heritage Malta manages 31 sites and museums[1] across Malta and Gozo, IT plays an important role in the management and conservation of sites and artefacts.

The ICT and Information Management unit maintains a number of packaged software applications, in-house applications and IT projects co-funded by the EU. The main IT systems used at Heritage Malta are:

- **Access Accounts** – The main accounting system used by the Finance Department within Heritage Malta.
- **Condition Assessment System** – A stand-alone electronic system with an on-line data entry form that was developed in-house for conservators to document the condition assessments of objects at Heritage Malta.
- **Hardware Inventory System** – An in-house web-based system which was developed to facilitate the ICT and Information Management unit to document and identify computers and users during support calls.
- **Heritage Malta Website** – The current website was developed by Heritage Malta and is currently being managed centrally by the ICT and Information Management unit. The latter have recently designed a new website and a first prototype was developed. The new website will eventually include a Content Management system and will be launched in the coming months.
- **Muses** – A web-based digital collection management system used to digitise and automate the artefact cataloguing processes. The aim of this application is to provide an easy to use and efficient tool to document objects, enriching them with Meta data and multimedia and to publish all the information online.
- **Plone** – An open-source content management software application which is being used by Heritage Malta as a local Intranet. The Heritage Malta Intranet was developed in adherence to recommendations from the Malta Information Technology Agency (MITA) and it is interoperable with other Intranets that are currently being used across Ministries.
- **Razuna DAM** – An open-source Digital Asset Management system and is built on open standards. The aim of this application is to centralise all the digital assets and manage and publish them independently from any format. It supports video, image, audio or document format which can be individually converted to other formats within Razuna.
- **Shireburn Payroll System** – The system provides a complete payroll processing of both full-time and part-time employees. This includes the maintenance of employee details through the management of leave, actual payroll calculation, printing of payroll reports and payslips, processing of direct credit payment and submission of periodical Final Settlement System (FSS) returns as required by the current legislation.
- **Shireburn Time and Attendance** – The system automates the capture and allocation of employee time and attendance information into the payroll system. The system was integrated with a Biometric Hand Reader installed in every site and museum.
- **Ticketing System (TIXPOINT)** – The system is used to sell admission tickets at Heritage Malta's sites and museums.

[1] All Heritage Malta Sites and Museums are listed in Appendix B

Chapter 1
Introduction

For the purpose of this IT audit, NAO will be evaluating the four major applications listed below:

- Condition Assessment System
- Hardware Inventory System
- Ticketing System (TIXPOINT)
- Muses – Collection Management System

1.5 Audit Scope and Objectives

The aim of this IT Audit is to collect and analyse evidence to determine whether Heritage Malta has the necessary controls to ensure that its IT and Information Systems maintain data integrity, safeguard assets, allow organisational goals to be achieved effectively and assist in making efficient use of agency's resources. This report includes the recommendations made by NAO to mitigate the potential risks identified in the IT audit.

The IT Audit was divided into three different stages:

- Initially, a pre-audit questionnaire was sent to Heritage Malta to gather the necessary information on the audit site prior to undertaking an on-site audit. The aim of the questionnaire was designed to familiarise the audit team with Heritage Malta and its IT setup prior to the audit visit.

- The second stage required a thorough understanding of Heritage Malta internal structures, functions and processes through a number of interviews with key officials and stakeholders. NAO also reviewed the latest strategic plan, annual reports, user manuals and other documents requested in the pre-audit questionnaire.

- The final stage examined how the IT applications are being used to achieve their objectives. In this regard, the IT Audit went through the processes and procedures related to every software application and checked whether these software applications were properly maintained. Furthermore, the IT Audit looked into the physical and logical access controls, adherence to policies, standards and procedures, network infrastructure, security controls, business continuity and disaster recovery plans.

To summarise all this, the objective of this report was:

- To gather all the relative information collected during the course of the IT audit.
- Verify whether the IT applications in use are being used efficiently and effectively.
- List all the findings and identify any potential risks.
- List all the recommendations to mitigate those risks.

1.6 Audit Methodology

To achieve the above objectives, a number of interviews were held with the Head of ICT and Information Management unit and other officials. Furthermore, a walk-through was held at Heritage Malta's Head Office, sites and museums to familiarise with the procedures of the different applications being used.

This audit report also makes reference to the Control Objectives for Information and related Technology (COBIT) 4.1 set of best practices which were listed in Appendix C. COBIT is a comprehensive set of resources that contains all the information organisations need 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 COBIT framework consists of four IT domains and 34 IT processes.

1.7 Structure of the Report

The report includes four further chapters each documenting the information collected and highlighting the findings and recommendations:

- Chapter 2 deals with IT management whereby Heritage Malta technology resources are managed in accordance with its needs and priorities.

Chapter 1
Introduction

- Chapter 3 reviews a selection of IT applications that are currently being used at Heritage Malta.

- Chapter 4 addresses the key components of information security and which security measures were implemented by Heritage Malta to maintain the confidentiality, integrity and availability of data.

- Chapter 5 analyses how Heritage Malta is managing and controlling its IT operations in the most effective way. Furthermore, it addresses whether Heritage Malta is confident with the business continuity or disaster recovery plans in the event of a service disruption.

1.8 Acknowledgements

NAO would like to express its thanks and appreciation to all the staff within Heritage Malta, particularly the Chief Executive Officer and the Head of ICT and Information Management unit and the staff who were involved in this audit, for their time, patience and assistance.

Chapter 2
IT Management

2.1 ICT and Information Management Department

The ICT and Information Management department has a number of functions within Heritage Malta and is currently divided into four different units:

- ICT Development and Maintenance
- Digitisation and Audio Visual Development
- Registry and Information Management
- Marketing and Communications

The ICT and Information Management department is headed by a manager who was appointed head of ICT in September 2005. In 2011, the Information Management department was added to the manager's portfolio. The manager holds regular meetings with his staff and reports directly to the CEO.

2.1.1 ICT Development and Maintenance Unit

The ICT Development and Maintenance unit is divided into two main components, namely the Information Systems and Software Development and the Infrastructure and ICT support.

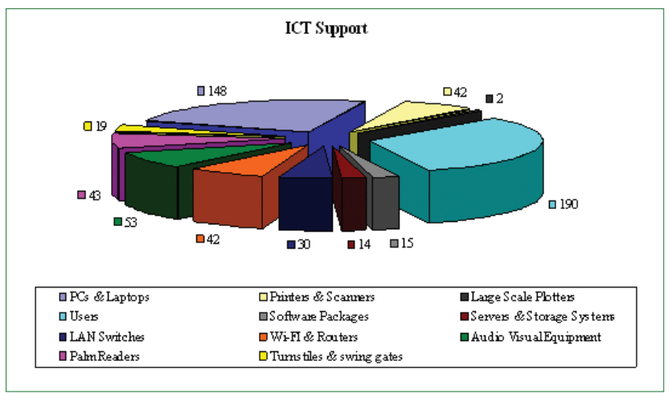


Figure 2

The Infrastructure and ICT support team is responsible for the day-to-day support and maintenance of all Heritage Malta's ICT equipment and packaged software applications. The unit was recently being managed by one IT Executive to support a number of users and ICT equipment as depicted in Figure two.

However, in 2011 Heritage Malta engaged an IT Co-ordinator to assist the IT Executive in his day-to-day operations.

The Information Systems and Software Development team develops and maintains a number of in-house applications. Such software applications include the Heritage Malta website, the Intranet, the Heritage Inventory system and the Collection Management Information system. The unit also assists in a number of EU funded programmes managed by European Institutions. These vary in content and objectives depending on the nature of the programme or project. Unfortunately, Heritage Malta only had one Senior Software Developer to manage all these applications. The Senior Software Developer also assisted the Infrastructure and ICT support team in any ICT related calls. The lack of resources within the ICT Development and Maintenance unit resulted in deficiencies in various projects entrusted to the Information Systems and Software Development team. In the last quarter of 2011, Heritage Malta engaged a Junior Software Developer to assist the Senior Software Developer with the development and maintenance of the current software applications.

2.1.2 Digitisation and Audio Visual Development Unit

The Digitisation and Audio Visual Development unit works closely with the ICT Development and Maintenance unit. The unit is divided into two, namely the Photography and Filming services department and the Audio Visual Development and Design department.

The Photography and Filming services department is made up of one person who is responsible for the digitisation of collections and for the creation of footage of any events being hosted in sites and museums. The footage is forwarded to the Audio Visual Development and Design department to create audio visuals which are then combined into high technology multimedia development and interactive systems. However, due to lack of resources, the filming role within this unit is no longer operative. This means that

Chapter 2
IT Management

this department is currently focusing on photography only to assist in the digitisation of collections and conservation which are then inputted into the Collection Management system and the outsourcing of the filming services.

Similarly, the Audio Visual Development and Design department is made up of one person. This department has successfully implemented a number of audio visual projects in a number of sites and museums, such as the War Museum, the Ħagar Qim visitors centre, the Inquisitor's Palace and the Ħagar Qim temple model audio visual. Given that the department is manned by only one person, the department can only work on one project at a time. If Heritage Malta intends to focus on the implementation of Audio Visual technology in all of its sites and museums, then one person may not be enough to cope with the current workload.

2.1.3 Registry and Information Management Unit

The Registry and Information Management unit is managed by one Senior Executive who is responsible for the Registry and Records Management and the Preservation and Management of Digital Assets. The Registry and Records Management unit was created in 2010 to deal with the archiving of information generated by Heritage Malta and to adhere to the Freedom of Information Act and the National Archives Act.

The setup of the Registry started with the filing and archiving of Human Resources paper based information and the archiving of a number of boxes left behind when the Head Office in Valletta moved to the current Head Office in Bighi. Every file or document was classified and stored according to its genre. All this manual process took quite a while to complete. Consequently Heritage Malta decided to implement a centralised records management application, to facilitate the filing and archiving of paper based information. Heritage Malta liaised with MITA for the implementation of the Document Registry (DocReg) application used across Government departments. The DocReg application assists the registry department in the movement of physical records, classification of files and documents and to provide a sequential reference number to every file or document.

The Preservation and Management of Digital Assets department processes large volumes of digital assets generated by all the departments within Heritage Malta. To date, there is over six Terabytes of information which has not been processed yet. Due to lack of resources, the digital asset management process was put on hold as the Senior Executive was assigned with the filing and archiving of information at the Registry and Records Management department.

2.1.4 Marketing and Communications Unit

The Marketing and Communications unit has a number of functions within the ICT and Information Management department. The unit focuses on public and media relations, internal communications, digital asset management, sales, marketing, patronage and sponsorships.

The public and media relations department is managed by one person who provides the public and the media with a better understanding of how Heritage Malta works. The department works with various facets of the media to promote forthcoming events within the various museums and sites and to inform reporters when something newsworthy takes place. These are communicated to the media and the general public through press releases, social media or over the Internet through Heritage Malta's website. Furthermore, a dedicated webpage has been created, namely http://heritagemalta.wordpress.com, whereby all the news and views related to Heritage Malta are posted on this page. On the other hand, all internal communication is disseminated on Heritage Malta's Intranet or Homepage. The department helps the head of the ICT and Information Management department in formulating policies and procedures related to public information programmes and to respond to requests for information, such as Parliamentary Questions or queries for the media.

The digital asset management department is involved in the development and maintenance of the Agency's corporate image and identity, which includes the usage of logos and signage. All the digital assets, such as photos, videos and other digital material are organised for internal and external use. This also includes the maintenance of digital content including related matter in social media sites. NAO observed that there is currently no one in the unit that is assigned duties relating to the area of organisation and distribution of digital assets. However, Heritage Malta engaged a number of part-time students to input all the digital assets into a centralised system.

The head of the Sales department co-ordinates the logistics involved in generating funds and to develop policies for collection and safeguarding of contributions. Apart from the revenue generated through the sale of tickets from sites and museums, Heritage Malta's basic revenue generation activities consists of sales of products from shops, the rental of assigned areas for private functions and the revenue generated from filming and photography.

The aim of the Marketing department is to run campaigns to promote Heritage Malta products, services and ideas. This comprises planning, advertising, product development, distribution and sponsorship. The Marketing department works closely with other departments to develop integrated marketing campaigns, organise surveys and to place adverts in the press and on the radio. Furthermore, it has a close working relationship with established operative stakeholders, such as Tour Operators, Malta Tourism Authority and Tourist Guides and manages the production of marketing materials, including leaflets, posters, flyers, newsletters and DVDs.

The Patronage and Sponsorships department provides the link between prospective patrons or sponsors and Heritage Malta. The department plans, implements and co-ordinates the necessary work to establish quality control guidelines for patron assistance. It also handles and negotiates patron requests in order to ensure focused customer care, certify that all agreed obligations are executed and draft sponsorship benefit contracts. NAO observed that the department is currently being managed conjointly by the Sales and the Marketing departments. However, NAO recommends that a dedicated person should be assigned to manage the Patronage and Sponsorships department.

The IT Audit determined that the ICT and Information Management department has a number of projects and initiatives on hold due to lack of human resources. This is hindering the ICT and Information Management department to function properly and achieve its objectives highlighted in Heritage Malta's Strategic Plan. NAO welcomes the fact that in the end of 2011, Heritage Malta drafted a human resources capacity plan for the recruitment of employees to fill in the vacant positions within the ICT and Information Management department.

Since most of the key functions within the ICT and Information Management department are dependent on one individual, NAO suggests that Heritage Malta should renew the present staff compliment and train the individuals to assist in the implementation of projects and initiatives highlighted in the Strategic Plan.

2.2 ICT Strategy

At the time of this IT audit, Heritage Malta did not possess a written ICT Strategy plan. However, the Head of ICT and Information Management department had proposed a plan based on industry standard organisation structures. The proposed plan aims to consolidate existing services, products and operational functions and intends to give a clear direction on the ICT and Information Management department's objectives, priorities and measures to be achieved.

NAO recommends that this proposed plan materialises and an actual ICT Strategy plan is drafted. The ICT Strategy should focus on creating and measuring business value from the investment implemented in ICT.

2.3 ICT Budget

As from 2009, Heritage Malta's financial period was changed to a calendar year ending 31st December. Heritage Malta finances its operations through revenues, mainly from admission fees to museums and sites, and also from a Government subsidy.

Heritage Malta seeks to upgrade and strengthen its core activities and operations so as to increase efficiency and thus reduce reliance on Government subsidy. In this respect, Heritage Malta managed to attract further funding from private sources, patrons and sponsors to help conclude various other projects.

The ICT budget allocated is determined on costings from the previous year and on new and ongoing projects highlighted in the strategic plan. In 2011, around 40% of the budget was allocated to new IT investment while 60% of the budget was allocated to IT Support.

Chapter 2
IT Management

2.4 Systems Development Life Cycle

The IT Audit went through the systems development life cycle that is being implemented by Heritage Malta and reviewed the processes involved in the planning, development, acquisition, testing, implementation and maintenance of software applications and the procurement, maintenance and disposal of hardware equipment.

2.4.1 Software Asset Management

During the course of this IT audit, NAO went through the project life cycle in terms of software asset management. NAO observed that the ICT and Information Management department adopted the conventional phases of the software development life cycle which is based on a systematic, sequential approach to software development. The software development life cycle that is being adopted by Heritage Malta is divided into seven different phases, which include:

- Feasibility Study
- Systems Requirements
- Conceptual Design
- Systems Development
- Systems Testing
- Systems Implementation
- System Maintenance and Support

Since a number of software applications were developed in-house, NAO examined the project life cycle that is being implemented by the ICT and Information Management department.

All in-house applications are planned using a strategic approach. Management develops a written long-term plan for systems that is strategic in nature. The plan may change over the months, but evidence exists that such planning pays dividends in terms of effective IT solutions over the long term. NAO observed that Heritage Malta's Strategic Plan 2011-2013 highlights one objective related to the project life cycle, namely:

"To make available IT Infrastructure and systems, access to records, shared information and knowledge".

NAO observed that Heritage Malta have allocated three dedicated servers for the development, testing and hosting of software applications. When an application is developed, the ICT and Information Management department carries out rigorous testing. Testing is carried out in different phases whereby all modules are tested individually and then, in conjunction with other modules, before they are tested in the enterprise system.

When the system is deployed, the ICT and Information Management department handles all systems documentation and user manuals. In this regard, NAO noticed that due to lack of resources, the ICT and Information Management department are doing its utmost to update all systems documentation and user manuals.

The ICT and Information Management department adheres to the change management process before any changes or updates are implemented on to the live environment. Initially, when a change or update is required, the department requests a written authorisation from management. When the change has been approved, all updates or changes are tested offline before being implemented to the live environment.

Heritage Malta procured a number of off-the-shelf software applications. While new hardware equipment is procured with a pre-installed operating system, all other Microsoft applications are procured through MITA as part of the Microsoft Enterprise Agreement. All the relevant software licenses are stored by the Stores and Logistics department in the accounts software application. NAO was informed that the latter was customised by the supplier as per Heritage Malta requirements whereby a number of add-ons were implemented into the system.

2.4.2 Hardware Asset Management

The ICT and Information Management department liaises with the Stores and Logistics department for the procurement of new IT hardware. The procurement of new IT hardware is planned in the beginning of the year whereby the ICT and Information Management department and the Human Resources department determine whether new employees will be recruited during the year. Furthermore, the ICT and Information Management department refer to the Strategic Plan and verify whether new IT hardware is required for new or ongoing projects.

Chapter 2
IT Management

Since Heritage Malta did not opt for the procurement of hardware through the Government's Personal Computer (PC) leasing scheme, the ICT and Information Management department, through the Stores and Logistics department, have to go through the whole hardware life cycle in terms of procurement, maintenance, support and the disposal of IT equipment.

Whilst going through the IT Audit process, NAO observed that in mid-2011, Heritage Malta issued a call for tender for the supply and delivery of IT equipment under the public procurement regulations. The tender document stipulates that all IT equipment is procured with a three year warranty. The supplier is required to provide and secure the provision of a reliable and regular after sales for a period of two years after warranty.

The ICT and Information Management department disposes all of its faulty IT equipment through the Stores and Logistics department. The latter will update its hardware inventory database and declare all the faulty IT equipment as written-off. Heritage Malta will then liaise with a third party supplier for the disposal of all faulty IT equipment in Civic Amenity Sites.

NAO observed that prior to the disposal of IT equipment, Heritage Malta removes data on a computer system or hard disk through the normal windows formatting. NAO recommends that Heritage Malta implement procedures to identify and erase the sensitive information and software inside computers, disks and other equipment or media that have been identified for disposal, so that deleted data may not be retrieved by any internal or third party .

2.5 Third Party Suppliers

In line with OPM Circular No. 29/2005, MITA being the ICT Agency for the Government of Malta, was entrusted with the provision of all core services to all Government and public sector entities.

The ICT services contract stipulates that MITA will provide Heritage Malta's Head Office with a Fibre Optic connection and a backup ADSL connection on to the Government Network also known as MAGNET. On the other hand, most of Heritage Malta's sites and museums are connected to the MAGNET through an ADSL or Cable connection.

The ICT services contract also covers the 24/7 monitoring carried out on the MAGNET.

The monitoring is performed on core Wide Area Network (WAN) equipment and core access switches on a proactive basis, in order to prevent potential ICT problems resulting in service downtime. An element of monitoring is performed on a reactive basis by servicing any ICT failures and unusual events to ensure service availability.

MITA also reached an agreement with Heritage Malta for the provision of a number of ICT Services including:

- Internet Browsing and filtering
- Electronic mail (E-mail)
- Standard Desktop Security Configuration Services, such as Anti-Virus and Spam filtering of E-mails via black lists and tagging
- Access to MITA's Service Call Centre for the reporting of incidents related to the above services
- First line support for the resolution of incidents reported to MITA's Service Call Centre regarding the above mentioned services.

The ICT services contract defines the service level agreements being offered whereby an incident or task is classified according to its priority level, which may be Critical, High, Normal or Low.

Heritage Malta had a service level agreement with Maltaticket to offer its services as the exclusive service provider of a secure, computerised ticketing system. The service agreement stipulates that any additions or changes to admission tickets or ticketing programmes are to be coordinated through and approved by Heritage Malta's ICT and Information Management department. Furthermore, Heritage Malta is to be provided with continuous and unlimited access to secure online reporting and accounting of sales of tickets in sites and museums managed by Heritage Malta.

The ongoing development of customised reports and functionality may be requested by Heritage Malta from time to time. These should be implemented within reasonable and specific time frames as requested by Heritage Malta.

Chapter 2
IT Management

The service agreement explained how the POS (Point-of-Sale) system was implemented in different phases across Heritage Malta's sites and museums. At the same time, Heritage Malta was co-ordinating training to its employees while the system was being implemented.

2.6 Network Infrastructure

Heritage Malta Head Office and most of its sites and museums are connected to the MAGNET. Whilst Heritage Malta Head Office is connected through a 10Mbps Fibre connection, most of its sites and museums are connected through an ADSL or Cable connection. NAO observed that the Head Office is also connected to an ADSL line. The ADSL connection has been provided by MITA to automatically connect the Head Office to the MAGNET in the event of a service disruption on the main fibre connection.

On the other hand, the Ħagar Qim and Mnajdra Temples in Qrendi and the Museum of Archaeology and the Folklore Museum at the Citadel in Gozo are connected to an external service provider. In this regard, these do not have access to Heritage Malta file servers but do have access to the ticketing system, the Government E-mail and have Internet access.

As part of the core services contract all WAN equipment and core access switches are monitored by MITA on 24/7. The network connectivity is monitored and maintained by MITA and notifies the ICT and Information Management department whenever there is a service disruption. On the other hand, the Local Area Network (LAN) infrastructure is being monitored by the ICT and Information Management department.

During the course of this audit, Heritage Malta provided NAO with a network diagram together with a hardware inventory list of all the equipment found inside Heritage Malta's server room. While reviewing the network setup, NAO observed that all networking equipment is connected to an Uninterrupted Power Supply (UPS). The latter are regularly tested by the ICT and Information Management department.

Heritage Malta is also equipped with two Worldwide Interoperability for Microwave Access (WiMAX) connections. One of the WiMAX connections is used by the ICT and Information Management department to offer remote support to sites and museums which are not connected to the MAGNET. This connection also offers public IP addresses to employees who wish to connect remotely to the MUSES Collection Management system from the comfort of their home.

Heritage Malta provides a secure Wi-Fi connection through the secondary WiMAX connection. The secure Wi-Fi connection is normally used whenever the Multi Activity and Leisure rooms in Bighi are rented for private functions.

Finally, the Head Office is also equipped with two mobile high-speed Internet connections, which are normally used in an emergency situation whenever there is a service disruption on an ADSL or Cable connection at Heritage Malta's sites and museums. These mobile high-speed Internet connections are not connected to the MAGNET.

Chapter 3
IT Applications

Heritage Malta invested in a number of IT applications to carry out its operations and to process and maintain the considerable amount of data that is being generated within every unit.

During the course of this IT audit and as mentioned earlier in Chapter 1, NAO has evaluated the four major applications listed below:

- Condition Assessment System
- Hardware Inventory System
- Ticketing System (TIXPOINT)
- Muses – Collection Management System

3.1 Condition Assessment System

Over the years, every artefact was being assessed by a conservator whereby its condition was being documented manually and stored in a file. This amounted to a large number of files which were being kept by the conservator in different sites and museums. In this regard, Heritage Malta felt the need to centralise all the current documentation and input every artefact's condition into a dedicated database. This was clearly identified in Heritage Malta's strategic plan whereby one of its objectives states:

"To conduct systematic conservation audits to determine the state of conservation of all Heritage Malta collections, prioritise conservation works and define achievable conservation management plans".

To meet the above objective, the ICT Development and Maintenance unit developed a web-based condition assessment system which is accessible by the Conservation Division through Heritage Malta's Intranet. The system is based on MySQL database and was developed using the prototyping methods. These methods allowed the end-users to evaluate the developer's proposals and reach agreement on the system requirements.

The Condition Assessment System was launched in the last quarter of 2011 and is currently being used as a pilot project at the National Museum of Archaeology in Valletta. At the moment, the system is being administered by the ICT Development and Maintenance unit who are constantly in touch with the senior conservators for any enhancements required to the system. The system is being hosted on one of Heritage Malta servers and is backed up twice a week according to Heritage Malta's backup procedure.

Even though the Condition Assessment System is still in its initial stages, NAO observed a few shortcomings to the system. To date, the system does not have any access controls in place and thus will not prompt the user for any login credentials to access the system. NAO recommends that the system is accessible through a login and a password and different user levels are in place. Furthermore, Heritage Malta should implement audit trails and any changes to the system or data are recorded.

NAO also noticed that there are no filtering options in the search functionality. As data is being inputted into the system, the current search functionality is likely to become too cumbersome to search for a particular item. In this regard, NAO recommends that filtering options are added to the system to facilitate the search functionality.

Following the above recommendations, NAO was informed that Heritage Malta integrated the Condition Assessment System with Active Directory whereby authorised users can now access the system through their local domain credentials. Furthermore, NAO was also informed that Heritage Malta enhanced the search functionality to include an advanced filtering option with a full text search functionality.

3.2 Hardware Inventory System

The Hardware Inventory System is an in-house web-based system which was developed by the ICT Development and Maintenance unit to facilitate the ICT Support team in their day-to-day operations especially when providing remote support assistance to the end user. The unit adopted the waterfall development model which is a sequential design process whereby progress is seen as flowing steadily downwards through the phases of conception, initiation, analysis, design, implementation, testing and debugging, installation and maintenance.

Chapter 3
IT Applications

The ICT Support team inputs all the relevant information pertaining to the hardware assigned to every individual within Heritage Malta. The ICT Support team liaises with the Stores and Procurement department and makes sure that the Hardware Inventory system is kept up to date.

The system keeps track of the network configuration settings and all the software applications installed on every workstation. The ICT Support team also inputs the full network path where important user data is being stored. The aim is to facilitate the recovery of data in the event that a file or folder restore is required.

NAO observed that even though the system is solely being used by the ICT Support team, every user has administrative rights to logon on to the system. NAO recommends that two different user levels are in place, whereby the user level account is used for the day-to-day operations while the administrative account is solely used for any enhancements or upgrades required on the system.

Whilst going through the system, NAO noted that the system stores the local administration credentials used on all workstations in clear text. NAO recommends that the local administration credentials are removed from the system and stored separately.

NAO observed that the Hardware Inventory System offers a very effective search functionality whereby any type of hardware or user can be easily found. The data can then be exported in a format compatible with commonly used spreadsheet applications.

3.3 Ticketing System (TIXPOINT)

In 2003, Heritage Malta launched a new ticketing system for its sites and museums. It provided a basis on which the agency could implement innovative management concepts for its sites. Apart from providing an improved service for Heritage Malta visitors, the ticketing system was necessary to curb the misuse and occasional abuse on the issue of manual tickets and to provide an audit trail for every ticketing transaction.

At that time, Heritage Malta opted for a new off-the-shelf application which was implemented in three different phases. The implementation of the system started at Heritage Malta's Head Office and the National Museum of Archaeology, followed by the War Museum and the Palace Armoury. Initially the ticketing system was installed as a stand-alone system at the different sites and museums. Eventually, all the sites and museums were networked with Heritage Malta's Head Office. Extensive training was also provided to users within Heritage Malta to get accustomed to the new ticketing system.

In 2007, Heritage Malta upgraded its ticketing system following a collaboration agreement with MaltaTicket. TIXPOINT, utilises a centralised network structure where all Heritage Malta's site and museum admissions can be ticketed on-site or online through its own website. Tickets can also be procured through MaltaTicket agents and a number of hotels in Malta and Gozo. In addition, local tour operators have been provided access to the TIXPOINT system to issue tickets from their own offices.

TIXPOINT, which was in use at the time of this IT audit but has now been replaced, brought a considerable change in the issue of tickets. The system introduced a number of multi-pass tickets which have made it possible for individual visitors to save money while visiting a number of Heritage Malta sites and museums. Compared to the previous application whereby one person purchasing a multi-pass ticket was in possession of more then one individual ticket, TIXPOINT offers the facility to issue one multi-pass ticket to cater for more then one site and museum. This translates into savings on paper and administrative work.

Tour operators who work closely with Heritage Malta welcomed TIXPOINT as it is more user-friendly and more efficient, saving tour operators, precious time and money in processing requests. Whereas previously tourist guides had to be in possession of individual tickets of different denominations for each person in the group, one sheet of paper is now enough to account for all the members of the group irrespective whether they are visiting one site or many.

The TIXPOINT system is accessible over the Internet through a secure connection. Every user who has been granted access to the system can type in their credentials through a virtual keyboard. Alternatively, the credentials can be typed in directly if the computer has a keyboard installed. NAO observed that there is no session time-out if the system is left idle. Moreover, even though the password can be changed at the user's discretion, it does not expire over a period number of days. In this regard, NAO recommends that Heritage

Malta liaises with Maltaticket to implement stricter access controls on the TIXPOINT system. Heritage Malta should consider implementing a two-factor authentication method, the user password should expire at least every 90 days and the system is locked if it is left idle over a period of 15 minutes.

Heritage Malta, through the ICT Development and Maintenance unit, liaises with Maltaticket for the management of the TIXPOINT user accounts. The Human Resources department notifies the ICT Development and Maintenance unit whenever a user is employed or terminates the contract with Heritage Malta. The ICT Development and Maintenance unit will then liaise with Maltaticket for the creation or deletion of an account. The same procedure applies whenever TIXPOINT user accounts are disabled for all the users who are on prolonged leave, career break or maternity leave.

Since user accounts are not being managed directly by Heritage Malta, the latter should keep tabs on the existing user accounts. Thus NAO recommends that Heritage Malta liaises with Maltaticket to periodically issue a detailed list on the number of active TIXPOINT user accounts. This will ensure that the existing user accounts correspond to the list of users who have been authorised by Heritage Malta to use the TIXPOINT system.

Through the Maltaticket website, a user can buy tickets for sites and museums and for any upcoming events in Malta such as concerts, sports or any other shows. The tickets can be procured by cash or locally drawn cheque. Credit or debit cards are also accepted against a minimal service charge. Furthermore the system offers other payment facilities, either through a post-paid billing arrangement with the promoter or operator of the event or through an account with the system, whereby tickets are procured from this account and the sales are then collected independently from the customer.

As part of business continuity, Maltaticket issued a number of manual tickets from the system. These manual tickets were distributed around Heritage Malta sites and museums and should only be used by Heritage Malta if the TIXPOINT system is unavailable. Since all manual tickets are enumerated sequentially with a bar code, every manual ticket issued should be scanned and inputted into the system once the TIXPOINT system is online again. All the manual tickets are audited by Heritage Malta's Finance department on a regular basis to prevent any misuse on the issue of manual tickets.

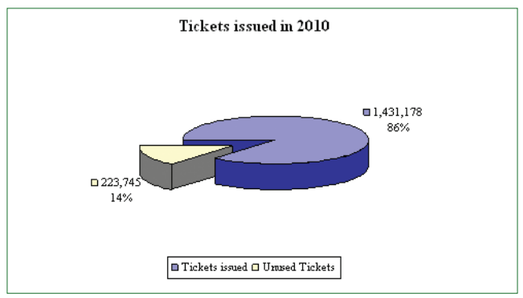


Figure 3

As depicted in Figure three, 1,431,178 tickets were issued in 2010, out of which 223,745 tickets were never used. The latter is attributed to multi-pass tickets that were issued but were never used within the 30 day time-frame window.

The TIXPOINT application can void tickets that were issued but were never used or void mistakes made whilst issuing tickets. The latter is normally done at the end of business day during the reconciliation process. The voiding of tickets is restricted according to the user levels. NAO observed that the TIXPOINT system offers three different user levels:

- The POS user level has access rights to sell tickets from a number of sites and museums.

- The Site Executive user level has access rights to sell tickets, to void tickets and view statistics on sales generated for the site or museum he/she manages.

- The Administrator user level is usually maintained by the Finance department within Heritage Malta. The Finance department has rights to monitor all the tickets issued in every site and museum. Furthermore, the Finance department can issue statistical reports on the sales generated from gift shops that are maintained by Heritage Malta and on the amount of audio guides that were leased to paying visitors.

Chapter 3
IT Applications

Heritage Malta had launched a membership scheme to encourage locals and permanent residents to make frequent visits to museums / sites and to acquaint themselves with the priceless treasures that a small island like Malta can offer. The membership scheme system was integrated with the TIXPOINT system whereby an individual can choose between an individual or family membership schemes at a very reasonable price. The membership scheme offers free unrestricted entry for the holder to all Heritage Malta sites and museums, valid for a period of 12 months from the date of issue, with the exception of the Ħal-Saflieni Hypogeum. The membership scheme entitles to a special 50% discount for tickets to Ħal-Saflieni Hypogeum, discounts on entry tickets to special exhibitions organised by Heritage Malta and discounts or special offers on purchases made in Heritage Malta museum shops.

During the course of this audit, NAO observed that the TIXPOINT system can generate different kinds of reports. All reports can be exported in a format compatible with commonly used spreadsheet applications to be able to perform data mining and analytics without the need to do major amendments on the report structure of the system. As depicted in Figure four, it is interesting to note that in 2010, the museum or site which attracted the most visitors was the Palace State Rooms, followed by the Ġgantija Temples, Ħagar Qim, the Palace Armoury and Tarxien Temples.

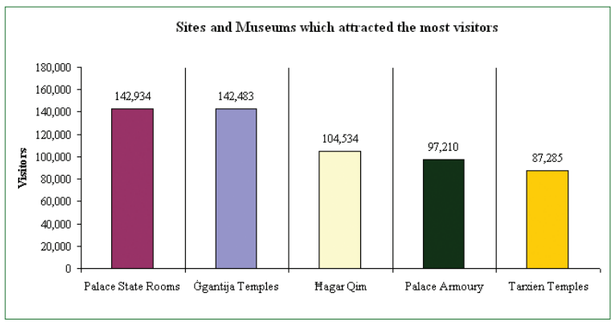


Figure 4

Every year, Heritage Malta plays a leading role during Notte Bianca in Valletta and Birgu Fest in Vittoriosa. During these events organised by the Malta Council for Culture and Arts and the Vittoriosa Local Council respectively, Heritage Malta's museums are open to the public free of charge or at a reduced price. As depicted in Figure five, during Notte Bianca, Heritage Malta attracted 17,292 visitors while the Birgu Fest attracted 7,742 visitors.

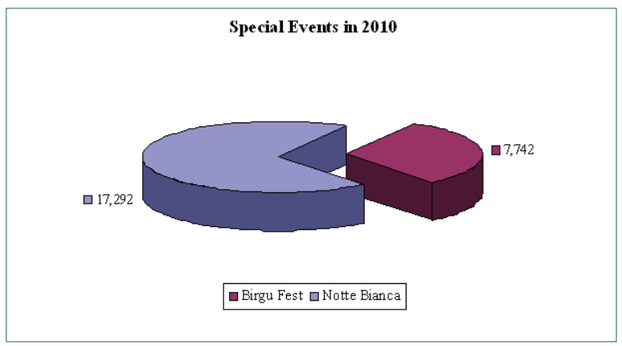


Figure 5

At the end of December 2011, Heritage Malta issued a statement whereby Maltaticket was no longer the official ticketing service provider. In this regard, a legal dispute is currently underway between Heritage Malta and Maltaticket. NAO would like to make it clear that the IT audit on the TIXPOINT system was carried out prior to this legal dispute and thus both this dispute as well as the new ticketing system that was not yet fully implemented by the writing of this report fall outside this audit's remit.

3.4 Muses – Collection Management System

Heritage Malta had purchased and assisted in the development of a customised cataloguing system code named Muses. This was highlighted in Heritage Malta's Strategic Plan 2011–2013 whereby one of its objectives states:

"To develop a systematic process for better and more effective collections management system".

This allowed Heritage Malta to catalogue its collections and artefacts according to international standards known as the Categories for Descriptions of Works of Art (CDWA), a product of the Art Information Task Force (AITF) funded by the J. Paul Getty Trust. CDWA describes the content of art databases by articulating a conceptual framework for describing and accessing information about works of art, architecture, other material culture, groups and collection of works, and related images..

Chapter 3
IT Applications

The Muses Collection Management system is a web-based application that is being used by cataloguers, researchers, students, curators and conservators to capture the information related to collections and artefacts in all Heritage Malta sites and museums. The system is an XML based schema that was built for interoperability between digital libraries. Every item that is inputted into the system is given a unique number which is then attached to an artefact for reference purposes. The system also captures digital assets of artefacts ranging from documents, images and videos in the format of PDF, TIFF, JPG, DWG and AVI/ MPEG file types.

All user accounts are managed by the ICT Development and Maintenance unit. The Human Resources department will notify the ICT Development and Maintenance unit whenever a new user wishes to gain access to the Muses Collection Management system. In contrast, all user accounts are deleted by the ICT Development and Maintenance unit whenever a user is no longer employed by Heritage Malta or is on prolonged leave, career break or maternity leave. NAO observed that user accounts do not expire over a period number of days and no password complexity is in place. In this regard NAO recommends that Heritage Malta implement stricter access controls on the Muses Collection Management system.

During the course of this audit, NAO observed that the Muses Collection Management system offers three different user levels:

- The Administrator is the top user level of the system. It has access to manage all user accounts and grant user permissions on specific modules in the system. The administrator can insert, update, select and delete a record or user account from the system.

- The Super user level is normally assigned to the curator and is only granted access to the data related to the museum under his/her supervision. Apart from approving the data inputted by the cataloguer, the super user can update an existing record or input new data into the system. The super user can also add or remove low resolution photos and videos and create cataloguer user accounts within the curator remit.

- The Cataloguer user level only has access to input the relevant data into the system.

In November 2011, a few enhancements were made to the Muses Collection Management system to facilitate the inputting of data and the searching functionality. Another enhancement was made to export data in a format compatible with commonly used spreadsheet applications. All the enhancements were made in a timely manner in collaboration between the ICT Development and Maintenance unit and the third party supplier.

Chapter 4
Information Security

Security failures can be costly to any organisation. Losses may be suffered as a result of the failure itself or costs may be incurred when recovering from an incident, followed by more costs to secure systems and prevent further failure.

Information security focuses on preventing attacks that target availability, such as a network disruption as a result of a denial of service attempt, and those that result in infections by malicious software, such as malware, that allow a third-party to gather sensitive information or gain unauthorised access to computer systems. This may result in theft, disclosure, modification or destruction of data.

NAO analysed the security measures that were implemented by Heritage Malta to maintain the confidentiality, integrity and availability of data.

4.1 Security Management

Security management is an ongoing process that entails formulating and following best practices and documentation. The process helps any organisation to document and classify the policies, procedures and guidelines to implement an effect security policy.

Even though a number of policies and procedures have been drafted by Heritage Malta, NAO recommends that Heritage Malta should have a minimal set of policies and procedures that classifies the information, the retention and storage of data, the disposal of information and the backup and recovery of data.

4.1.1 Information Classification

During the course of this IT audit, NAO observed that Heritage Malta generates a great amount of data. This data is being used within the different departments in their day-to-day operations and is easily accessible over the network.

NAO recommends that Heritage Malta should define an information classification policy. To begin with, Heritage Malta should evaluate whether the data being used is for internal or external use and whether it can be used for public dissemination or controlled distribution. Once a policy is defined, Heritage Malta would classify the data with regards to type of use and level of confidentiality.

Whilst going through the classification process, Heritage Malta would determine whether the information must be retained or reviewed. The review process establishes whether the information must be retained or can be disposed of. This process can significantly reduce the amount of information that requires special storage within Heritage Malta.

4.1.2 Information Retention and Storage

An information retention and storage policy would determine how information is stored and how long it is retained. This policy would identify who is the owner of every piece of information. In theory even though Heritage Malta adopts the above policy, NAO recommends that this policy is formalised.

During the course of this audit it became evident that there are large amounts of data which Heritage Malta must retain. Most of this data is composed of images or videos of artefacts that are either being exhibited in Heritage Malta's sites and museums or artefacts which are under conservation.

4.1.3 Disposal of Information

NAO recommends that Heritage Malta should define and implement procedures to prevent access to, or loss of, sensitive information and software from computers, disks and other equipment or media when they are stored, disposed of or transferred to another user. NAO were informed that Heritage Malta makes reference to the National Archives Act when disposing of IT equipment which may contain sensitive information.

NAO observed that the ICT Development and Maintenance unit removes data on a computer system or hard disk through formatting. This process does not guarantee that the data can be retrieved from a hard disk after being deleted through third party software.

NAO recommends that Heritage Malta implement procedures to identify and erase the sensitive information and software inside computers, disks and other equipment or media that have been identified for disposal so that deleted data may not be retrieved by any internal or third-party. Care must be taken to meet the requirements of data protection and to protect the confidentiality of data when a machine is transferred to another user. The original user should remove any personal data that is not confidential by nature. If previously held data

Chapter 4
Information Security

is considered as sensitive, NAO recommends that the disk is reformatted and then a secure wipe of the disk should be carried out with appropriate software.

Following the above recommendation, Heritage Malta informed NAO that action has been taken to format and secure wipe hard disks targeted for disposal.

4.1.4 Backup and Recovery of data

Every organisation which uses IT and data in their operations should adopt a backup and recovery plan. The plan should enable the organisation to recover lost data and to recover computer operations from loss of data. This might entail a simple restore of lost or corrupted data or a full system restore due to a hardware malfunction or a complete loss of computer operations as a result of a fire

NAO observed that a backup procedure is in place whereby all Heritage Malta servers are being backed up over the network on to a Network Area Storage (NAS) device. During the week, an incremental and a full system backup is scheduled on every server while a full system monthly backup is scheduled at the end of the month.

NAO observed that the ICT Development and Maintenance unit monitors every server backup on a daily basis and records every backup log in a dedicated file. Test restores are periodically taken to validate that the backup process is reliable and ensures that the process is actually recording all of the data onto the NAS storage device.

Even though the NAS storage device has been configured with a redundant array of hard disks, Heritage Malta has two mirrored NAS storage devices to backup all Heritage Malta servers. If Heritage Malta suffers a widespread disaster such as a fire, the event would destroy the backup data as the NAS storage devices is currently being hosted in Heritage Malta's server room. The backup principle for storage is to provide a location that is at a safe distance from the server room. Thus NAO recommends that Heritage Malta either finds an alternate location to the current NAS storage devices or replicate the data from the device on the second NAS storage device located in a safe distance from the server room.

Based upon NAO recommendations, Heritage Malta intends to re-allocate the secondary NAS storage device in a different location.

4.2 Identity and Access Management

Identity and access management is the process of establishing and proving one's identity and the resources they can access. The aim is to prevent unauthorised access to data, unauthorised use of system functions and programs, unauthorised updates or changes to data, and to detect or prevent unauthorised attempts to access computer resources. In this regard, NAO observed how the ICT Development and Maintenance unit adopted these processes within Heritage Malta and what measures were being taken.

4.2.1 Authentication

Authentication is the process used to verify the identity of a person or entity. This is achieved by providing every user with a login and a password. The login is uniquely identifiable and is always assigned to the individual.

NAO observed that the ICT Development and Maintenance unit processes all user accounts. The unit liaises with MITA for the creation of Government E-mail and Internet accounts to every Heritage Malta user. On the other hand, if a user wishes to gain access to a particular folder or application hosted on Heritage Malta servers, a written approval by his/her superior is required. The unit will then create the necessary accounts and inform the user accordingly.

During the course of this IT audit, NAO observed that the ICT Development and Maintenance unit accesses all Heritage Malta servers through the default administrator account. NAO recommends that all default accounts are removed and replaced by uniquely identifiable accounts with the same privileges as the default administrator accounts. The default administrator account should only be used in an emergency situation. Furthermore, privileged access activity must be regularly reviewed and suspicious events should be investigated.

In this regard, the ICT Development and Maintenance unit must ensure that adequate storage space and memory is allocated on every Heritage Malta server for access logs. Furthermore, all logs should record who, what, when, where and how resources were accessed over the network.

4.2.2 Password Management

Passwords are a primary means to control access to systems and should therefore be selected, used and managed to protect against unauthorised discovery or usage.

Passwords provide the first line of defence against improper access and compromise of sensitive information.

To enhance the level of security, NAO observed that a number of measures were implemented by the ICT Development and Maintenance unit. The password history has been enforced in conjunction with the minimum password age policy setting adopted by MITA, to ensure that old passwords are not continually reused. In this regard, the policy has been set on all Heritage Malta domain accounts to a minimum of five passwords before an old password can be reused.

A minimum password length policy has been defined so that users cannot make use of blank passwords, and users must create passwords with a minimum of eight characters in length. Furthermore, the password must meet the complexity requirements policy setting. The policy checks all new passwords to ensure that they meet basic strong password requirements, which include a mix of letters, numbers and symbols.

Almost every user password, including the Government E-mail and Internet passwords, expires every 90 days. Users can change their password prior to expiration or whenever users have forgotten their password. In this case, every user has to notify the ICT Development and Maintenance unit to change their password. The unit has sufficient privileges to reset most of the passwords and to unlock the login ID when necessary. Whenever the ICT Development and Maintenance unit resets a password, the user must change password upon first logon.

During the course of this IT audit, NAO observed that the ICT Development and Maintenance unit does not store any administrator passwords. NAO recommends that the current and previous administrator passwords are stored and kept separately in a sealed envelope and should only be accessible by authorised personnel within Heritage Malta.

Based upon the above recommendation, Heritage Malta informed NAO that administrator passwords are being stored in a secure safe.

4.2.3 Information Access Control

Authorised users should be constrained from having access to all data and applications. Heritage Malta users should only have access to those applications necessary to do their particular job. That limitation also includes data access rights of read-only, read/write or no access where applicable.

NAO observed that Heritage Malta has adopted an effective and logical approach to link access control to human resources procedures. When an employee is hired, transferred or leaves Heritage Malta, the human resources department liaises with the ICT Development and Management unit and triggers the procedures to include the required changes to that employee's access rights.

In the case of new employees, access rights are granted only to those applications and data necessary for that person's job responsibilities. In this regard, the ICT Development and Maintenance unit only grants full access to a user on his/her personal folder and read/write access on shared folders residing on Heritage Malta Office Automation (OA) server. Similiarly, if an employee is transferred those access rights may change depending on the different responsibilities associated with the new job role.

Upon termination of employment, the Human Resources department sends all the necessary information by E-mail to the ICT Development and Maintenance unit. In return, the unit backs up all the data residing on the workstation and server, revoke all access rights that were previously granted on Heritage Malta OA server and delete the user account from Heritage Malta's domain. Furthermore, the ICT Development and Maintenance unit will liaise with MITA for the deletion of E-mail and Internet accounts.

4.2.4 Auditing

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.

NAO notes with satisfaction that Heritage Malta has adopted security auditing on all windows servers. The security log contains records of valid and invalid logon attempts and events related to resources use, such as creating, opening or deleting files.

Chapter 4
Information Security

Heritage Malta should ensure that adequate storage space and memory has been allocated on every server for the storage of audit logs. Furthermore, strong access controls should be in place to help prevent unauthorised access or manipulation to audit logs. Since audit logs are stored locally on every machine, NAO recommends that the ICT Development and Management unit periodically stores security audit logs remotely on to a storage device.

4.3 Security Awareness and Training

Security awareness should be of an ongoing process that seeks to ensure that all users are familiar with the information security policies and best practices that govern the use of IT assets. NAO recommends that the policies and best practices should be disseminated through Heritage Malta's normal communication channels to be effective. Communication and awareness help ensure that information is conveyed to the appropriate users in a timely manner.

During the course of this IT audit, NAO observed that a number of Heritage Malta users are not familiar with any security threats they might come across in their day-to-day operations. NAO recommends that Heritage Malta establishes a process in place to concisely and clearly explain basic information security principles and best practices in the use of its IT assets over and above the Security Awareness Campaign that was adopted by MITA across all government departments and entities.

In this regard, NAO recommends that all Heritage Malta employees should receive appropriate training and regular updates to foster security awareness and compliance with security policies and procedures. Security awareness should also be included in the induction training for new employees.

Following the above recommendations, NAO were informed that Heritage Malta plans to draft an IT Handbook which will make reference to IT security related policies. Eventually this will be distributed to new employees and all existing users within Heritage Malta.

4.4 Anti-Virus Software

To effectively control and prevent the spread of malware, an organisation should adopt reliable Anti-Virus software across its network infrastructure. NAO observed that the ICT Development and Maintenance unit liaised with MITA to replace the Anti-Virus software installed on all servers and workstations across Heritage Malta, with Symantec Endpoint Protection (SEP).

SEP integrates essential security technologies in a single agent and management console. Besides an Anti-Virus and Anti-Spyware product, SEP incorporates an Intrusion Prevention System (IPS), Firewall and Application and Device Control. Furthermore, SEP prevents any workstation from connecting to more than one network simultaneously thus eliminating the risk of network bridging.

NAO observed that SEP has been successfully deployed on almost all Heritage Malta's servers and workstations. However, there are still a number of workstations which still have the previous Anti-Virus software installed. In this regard, NAO recommends that the ICT Development and Maintenance unit requests a report from MITA to establish which workstations still have the previous Anti-Virus installed.

The Symantec Endpoint Protection software is updated automatically by MITA. The latter manages all the endpoints and provides all the necessary support, maintenance and updates. MITA sends a periodic report to the ICT Development and Maintenance unit of any server or workstation which has been infected with a virus or which has not been updated with the latest virus definitions.

4.5 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.

Chapter 4
Information Security

Operating system manufacturers usually provide regular product updates. These are classified as security updates 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 Windows users. There are mainly three different kinds of updates:

- Hotfixes are used to make repairs to a system during normal operation, even though they might require a reboot. This allows the system to continue normal operation until a permanent repair can be made. Microsoft refers to a bug fix as a hotfix. It involves the replacement of files with an updated version.

- A service pack is a comprehensive set of fixes consolidated into a single product. It may be used to address a large number of bugs or to introduce new capabilities in an Operating System. When installed a service pack usually contains a number of file replacements.

- A patch is a temporary or quick fix to a program. Patches may be used to temporarily bypass a set of instructions that have malfunctioned. Unfortunately a patch may add the potential for new problems. Most manufactures would rather release a new program than patch an existing program.

To mitigate risks related to malware and security exploits, NAO observed that the ICT Development and Maintenance unit adopts two different approaches when applying patch management on servers and workstations. While all workstations have been configured to automatically download and install product updates through the Microsoft Windows update tool, the ICT Development and Maintenance unit deploy product updates manually on servers.

The ICT Development and Maintenance unit ensures that the server was backed up successfully, prior to installing a security or critical update on a server. Initially, a hotfix or service pack is deployed on a testing server. If there is no abnormal behaviour, the hotfix or service pack is deployed on the remaining servers.

NAO observed that the ICT Development and Maintenance unit is regularly informed by MITA with a list of hotfixes or service pack that needs to be installed on a particular server or workstation.

Chapter 5
IT Operations

Continuity of operations and correct functioning of information systems are essential in any organisation. Threats to computerised information and processes are threats to business quality and effectiveness.

In this regard, NAO reviewed whether Heritage Malta is managing and controlling its IT operations in the most effective way to maintain data integrity and to ensure that the IT infrastructure can resist and recover from errors and failures.

5.1 Data Centre Security Controls

During the course of this IT audit, NAO examined whether physical access and environmental controls are in place to safeguard the number of servers and networking equipment being hosted in Heritage Malta's server room.

5.1.1 Physical Access Controls

Physical access controls are designed to protect the computer hardware, software and network equipment from damage, theft and unauthorised access. In this regard, NAO analysed the physical access controls found in Heritage Malta's server room and whether access is restricted to those who need to maintain the servers or infrastructure of the room and in an emergency situation after office hours.

Heritage Malta's server room is accessible through an adjacent room where the ICT Development and Maintenance unit stores a number of user manuals and old or faulty computer hardware. Authorised users can gain access to both rooms through a key. In an emergency situation, the security personnel on duty have access to both rooms after office hours. NAO observed that Heritage Malta could not guarantee that only authorised users have access to these rooms. Thus NAO recommends that stricter access controls are in place to protect Heritage Malta from unauthorised access to the server room.

In interim, NAO suggests that Heritage Malta replaces the server room door locks and all the keys are kept by security personnel. Only authorised users can request the key from the security personnel to gain access to the server room and must also sign on a logbook indicating the name, date and time of entry and departure and reason for visiting.

Physical access controls can be enhanced by implementing combination door locks whereby a numeric key pad is installed at the door to gain entry. The combination must be changed at regular intervals by the individual or whenever an authorised user is transferred, resigns or subject to disciplinary action. This reduces the risk of the combination being known by unauthorised users.

Another option is to implement electronic door locks whereby a magnetic or embedded chip-based plastic card must be placed in front of a sensor reader to gain access to the server room. Every card is assigned to an identifiable individual who has been authorised by management to access the server room. The card can be easily deactivated in the event that the card is lost or stolen or the user no longer requires access.

NAO observed that even though a visitor's log book is available at Heritage Malta's reception desk, the server room does not have a log book in place. If a third-party supplier is called in by Heritage Malta to carry out maintenance or repairs inside the server room, NAO recommends that the supplier signs on the log book indicating their name, company representative, reason for visiting, and date and time of entry and departure. While maintenance or repairs are underway the supplier must be accompanied by authorised users at all times.

Even though the server room is equipped with a Closed Circuit Television (CCTV) camera, the ICT Development and Maintenance unit did not confirm whether the CCTV camera is operational. NAO observed that there are no signs indicating that a CCTV camera is operational before entering the server room. NAO recommends that Heritage Malta installs more then one CCTV camera. These must be located at strategic points and monitored by authorised users. The CCTV recordings must be saved and should be retained for possible future playback. Access to the live and recorded images should be restricted to authorised users only.

NAO noticed that the server room is not equipped with any intruder alarm. NAO suggests that an alarm system is installed and motion detectors are placed in strategic points. After office hours, security personnel on duty should be able to hear the alarm when activated.

Chapter 5
IT Operations

5.1.2 Environmental Controls

Environmental exposures should be given the same level of protection as the physical exposures. Environmental exposures are due primarily to naturally occurring events such as lightning, flooding, fire, electrical interruption and other environmental disasters. During the course of this audit, NAO examined whether the server room has any environmental controls in place and what measures are being taken to mitigate these risks.

NAO observed that the server room does not have any smoke detectors or a fire suppression system in place. A fire may cause a considerable amount of damage to the building and hardware equipment if it is not detected immediately. In this regard, NAO recommends that smoke detectors are installed inside the server room and connected to a central fire alarm system. The latter are powered by the main electrical distribution and backed up with a battery power. If smoke is detected inside the room, it will produce an audible alarm when activated. Smoke detectors should then be inspected and tested annually by a local supplier.

Alternatively NAO suggests that a fire suppression system is installed to automatically activate immediately after detection of high heat, typically generated by fire. Appendix D depicts the different fire suppression systems in use in server rooms.

If a fire suppression system or smoke detectors are installed inside the room, NAO recommends that the server room is equipped with an alarm control panel. The latter is the controlling component of a fire or smoke alarm system. Alarm control panels are systems which receive information from environmental sensors, such as smoke detectors, process the information and then trigger an audible alarm. Whenever the alarm is raised, this can be acknowledged or silenced from the panel. In the event of a power disruption, an alarm can still be triggered as the panel is backed up with batteries.

As a precautionary measure, NAO observed that the server room is equipped with two fire extinguishers. These are serviced once a year and inspected by a local supplier. Furthermore, a number of fire extinguishers are placed in strategic locations within Heritage Malta Head Office.

NAO noticed that the server room does not have any computer raised flooring and the network cables are exposed and placed haphazardly behind the network cabinets. To mitigate against electrical fires, the network cables should be placed in fire-resistant panels or conduit and ideally laid under a computer raised floor. Furthermore, NAO recommends that the server room is cleared from two filing cabinets and boxes and placed in the adjacent room. A warning sign should be placed at the door marking the room as restricted access and prohibiting food, drink and smoking inside the server room.

In the event of a power failure, the main networking equipment and the three main servers are connected to different UPS's. NAO observed that the remaining PC servers are not connected to a UPS. However, Heritage Malta is in the process of procuring three new UPS. These will be procured with a network management card for secure monitoring and control of the UPS via a web browser. The network management card will then be configured to send an E-mail notification to the ICT Development and Maintenance unit in the event of a power disruption. The servers that will be connected to these UPS will be installed with UPS software which will trigger an unattended shutdown when a power failure is detected.

Since the main servers have dual power supplies, NAO suggests that the servers are connected to different UPS's. In the event of a hardware malfunction on one of the UPS's, the servers will remain switched on as the load will be shifted on the remaining UPS.

NAO observed that the server room is equipped with only one air condition unit. As part of its business continuity, if the air condition unit malfunctions, Heritage Malta has a number of portable air condition units available until the main air condition unit is repaired.

Even though the air condition unit is being monitored daily by the ICT Development and Maintenance unit, NAO recommends that a temperature and humidity monitor is installed inside the server room to determine if the temperature and humidity levels are adequate

Following the above recommendations, NAO were informed that Heritage Malta installed two data loggers to monitor the temperature and humidity levels inside the server room.

5.2 IT Service Management

IT Service Management (ITSM) practices are important to provide assurance to Heritage Malta users and management that the expected level of service is being delivered.

Incident management is one of the critical processes in ITSM. Incident management focuses on providing increased continuity of service by reducing or removing the adverse effect of disturbances to IT services. In addition to incident initiation, other steps include the classification of incidents, escalation of incidents to third party suppliers, resolution and closure of incidents.

Incident management is reactive and its objective is to respond to and resolve issues as quickly as possible. It is essential for any incident handling process to prioritise items after determining the impact and urgency. NAO observed that the ICT Development and Maintenance unit keeps track of all incidents in a centralised spreadsheet, whereby a colour code scheme is used to determine the current status of an incident, namely:

- Red – The incident is given high priority and requires immediate attention.
- Amber – The incident is being seen to or is currently on hold.
- Green – The incident was resolved and marked as completed.

Unresolved incidents are normally escalated to third-party suppliers especially if it is hardware related. NAO observed that Heritage Malta procures most of its hardware with a three year warranty. Moreover, the third-party suppliers are bound to provide reliable and regular after-sales service and provide spares for all items for a period of two years after warranty.

Even though the ICT Development and Maintenance unit keeps track of all incidents, the spreadsheet cannot correlate incidents which are similar in nature to identify the root cause. In this regard, NAO observed that the ICT Development and Maintenance unit is looking into the possibility of developing an in-house application to streamline the current incident management process and facilitate the problem management process.

Problem management aims to resolve issues through the investigation and in-depth analysis of a major incident, or several incidents that are similar in nature, in order to identify the root cause.

Once a problem is identified and the analysis has identified the root cause, the condition becomes a *"known error"*. A workaround can then be developed to address the error state and prevent future occurrences of the related incidents.

Problem management and incident management are related but have different methods and objectives. Problem management's objective is to reduce the number or severity of incidents, while incident management's objective is to return the effected business process back to its "normal state" as quickly as possible. NAO observed that if Heritage Malta adopts problem management, the end result will show a significant improvement in the quality of service being offered by the ICT Development and Maintenance unit and will eventually minimise the impact on Heritage Malta business process.

As depicted earlier in Chapter two, the ICT Development and Maintenance unit adheres to change management process in the software development life cycle process. This is achieved by formalising and documenting the process of a change request, obtain a written authorisation, carry out the necessary testing, implement the change request and finally communicate to the respective users when the change is completed.

NAO observed that the ICT Development and Maintenance unit adopts to some extent a change management process when developing or maintaining an in-house software application. However, the ICT Development and Maintenance unit is not in total conformity with the change management best practices as not all changes were documented or updated. In this regard, NAO recommends that every change management process is properly documented or updated prior to implementation and easily available for any future reference.

Chapter 5
IT Operations

5.3 E-mail and Internet Services

Today E-mail and Internet services are considered as mission critical services in any organisation, for the exchange of information and business decision making. However, E-mail and Internet services are subject to rules that are appropriate and similar to a paper-based work environment.

E-mail has become an important component in any office automation system. E-mail facilitates the exchange of information, speeds up the decision making process and reduces paperwork, resulting in increased productivity, reduces costs and ensures better delivery of services.

Heritage Malta's E-mail and Internet services are being provided by MITA through the government's communications backbone, MAGNET. In this regard, NAO observed that Heritage Malta has adopted the Electronic mail and Internet services directive that was issued by the former Central Information Management Unit (CIMU) in 2003. NAO noted that this policy has been included in the Government of Malta Information and Communication Technology (GMICT) Policy Roadmap 2010-2012 whereby it will be reviewed by MITA and will be re-issued shortly.

NAO observed that every Heritage Malta user was provided with a government E-mail and Internet account. 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 other users within Heritage Malta.

Similiarly, every user is responsible and held accountable for Internet activities done. Even though an adequate filtering technology is being used by MITA, to prevent access to illegal material, every user should ensure that his/her account remains secure and not disclose the password or use someone else's password.

MITA maintains the right to monitor the volume of Internet and network traffic, together with Internet sites visited. The specific content of any transaction will not be monitored unless there is a suspicion of improper use. In addition, an E-mail sent through the MAGNET 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. To this effect, any attempt to send or cause such counterfeit E-mail to be sent to or through the MAGNET is unauthorised.

NAO suggests that Heritage Malta should periodically notify its employees on the relevant points highlighted in the electronic mail and Internet services directive especially the restrictions on use of E-mail and Internet services as depicted in Appendix E.

5.4 Risk Management

During the course of this IT audit, NAO observed that Heritage Malta does not have a formal business continuity and disaster recovery plan in place. However, if the ticketing system is unavailable due to power disruption or network connection failure, Heritage Malta have implemented a contingency plan on the issue of manual tickets or to make use of a third-party Internet dongle instead. On the other hand, the Stores and Logistics department stocks a number of hardware spares to repair or replace critical hardware equipment.

In this regard, NAO suggests that a Business Impact Analysis and a Risk Assessment exercise are performed from which a Business Continuity and Disaster Recovery plans can be achieved as represented in Appendix F.

5.4.1 Business Impact Analysis

A Business Impact Analysis (BIA) is a critical step in developing a Business Continuity Plan (BCP). The purpose of the BIA is to identify the various incidents or events that could impact the continuity of operations and the financial, human, legal and reputational impact on Heritage Malta. The BIA will identify how quickly essential business units and/or processes have to return to full operation following a disaster situation.

The BIA process is based upon the information collected from senior management and key persons within Heritage Malta. The information can be collected using different kinds of approach. One of the popular approaches is the questionnaire approach whereby a detailed questionnaire is circulated to key users in IT and to the end-users. Another alternative is to interview groups of key users. The information gathered during these interviews or from

Chapter 5
IT Operations

the questionnaire response is tabulated and analysed for developing a detailed BIA plan and strategy.

In this regard, NAO recommends that Heritage Malta lists and reviews its critical and non-critical functions. For each critical function, Heritage Malta should then determine:

- Recovery Point Objective (RPO) – the acceptable data loss in case of disruption of operations. It indicates the earliest point in time in which it is acceptable to recover the data.

- Recovery Time Objective (RTO) – the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations must resume after disaster.

After going through this process, Heritage Malta should determine a recovery strategy to identify the best way to recover a system or critical function in case of interruption, including disaster, and provide guidance based on which detailed recovery procedure to be adopted.

5.4.2 Risk Assessment

Apart from the BIA, Heritage Malta should carry out a risk assessment to analyse the value of its assets, identify threats to those assets and evaluate how vulnerable each asset is to those threats. The latter may be caused by natural causes, such as floods, thunderstorms and fire or caused by human beings, such as hacking attacks and virus or human errors. A disruption in service caused by system malfunctions, accidental file deletions, network denial of service (DoS) attacks, intrusions and viruses can be classified as a threat to Heritage Malta's daily operations. In this regard, a restoration of hardware, software or data files is required to recover operational status and resume service.

In this respect, NAO suggests that a risk analysis will define preventive measures to reduce the probability of these threats occurring and to identify countermeasures to successfully deal with these constraints if and when they develop. Therefore, a well-defined, risk-based classification system needs to be in place to determine whether a specific disruptive event requires initiating a BCP or a disaster recovery plan (DRP).

5.4.3 Business Continuity Plan and Disaster Recovery Plans

The primary objective of a BCP is to protect Heritage Malta in the event that all or parts of its operations and/or information systems are rendered unusable and to help Heritage Malta to recover from the effect of such events.

The BCP defines the roles and responsibilities and identifies the critical IT application programs, operating systems, networks, personnel, facilities, data files, hardware and time frames needed to assure high availability and system reliability based on the inputs received from the BIA and Risk Assessment exercise.

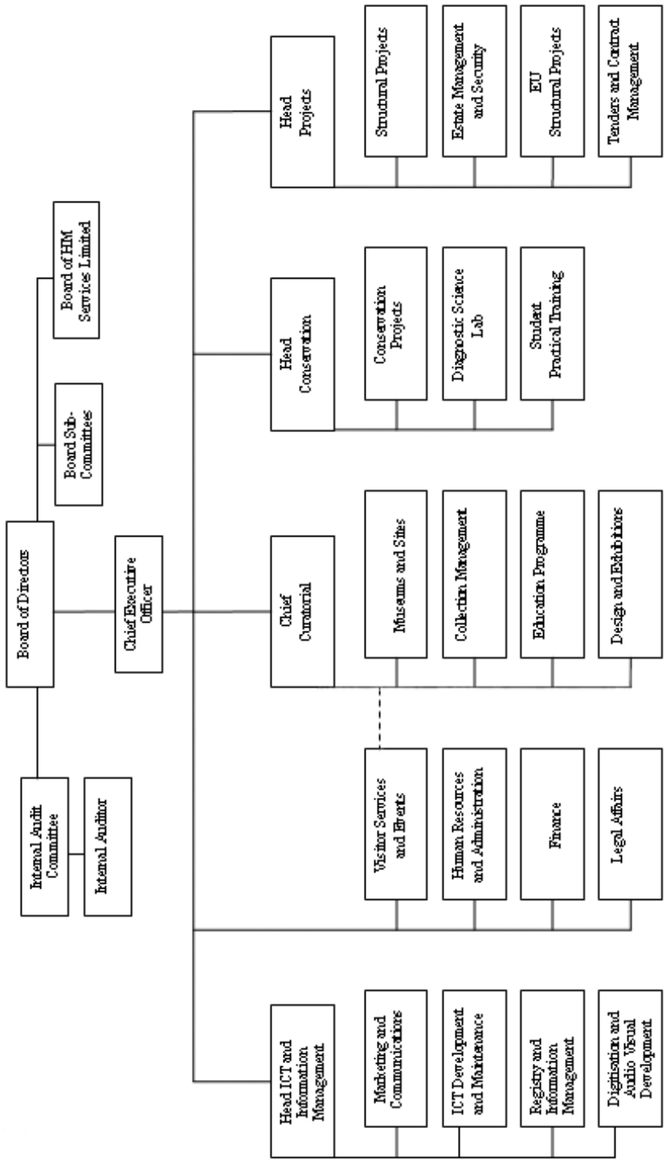
While a BCP refers to the activities required to keep Heritage Malta running during a period of interruption of normal operation, a DRP is the process of rebuilding the operations or infrastructure after the disaster has passed.

A DRP is a key component of a BCP, and refers to the technological aspect of a BCP, which includes the advanced planning and preparations necessary to minimise loss and ensure continuity of critical business functions in the event of a disaster. A DRP comprises consistent actions to be undertaken prior to, during and subsequent to a disaster.

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 is invoked. This will evaluate the effectiveness of the recovery documentation and establish whether the recovery objectives are achievable. The end result is to identify any improvements required in the DR strategy, infrastructure and the recovery processes established in the DRP.

Appendices

Appendix A – Organisation Chart



Appendix B – Heritage Malta Sites and Museums

Malta

1. Borġ in-Nadur – Birżebbuġia.
2. Għar Dalam Cave and Museum – Birżebbuġia.
3. Għajn Tuffieħa Roman Baths – Għajn Tuffieħa.
4. San Pawl Milqi – Għajn Tuffieħa.
5. Tas-Silġ – Marsaxlokk.
6. National Museum of Natural History – Mdina.
7. Ta' Ħaġrat and Ta' Skorba Temples – Mġarr.
8. Tal-Mintna Catacombs – Mqabba.
9. Ħal-Saflieni Hypogeum – Paola.
10. Ħaġar Qim Temples – Qrendi.
11. Mnajdra Temples – Qrendi.
12. Abbatija tad-Dejr, Rabat.
13. Domus Romana – Rabat.
14. St. Paul's Catacombs - Rabat.
15. Tarxien Temples – Tarxien.
16. National Museum of Archaeology – Valletta.
17. National Museum of Fine Arts – Valletta.
18. National War Museum – Valletta.
19. Palace Armoury and State Rooms – Valletta.
20. Part of Fort St.Elmo – Valletta.
21. Tal-Pillar Church – Valletta.
22. Fort St.Angelo – Vittoriosa.
23. Inquisitor's Palace – Vittoriosa.
24. Malta Maritime Museum – Vittoriosa.

Gozo

1. Museum of Archaeology – Citadel, Victoria.
2. Folklore Museum – Citadel, Victoria.
3. The Old Prison – Citadel, Victoria.
4. Museum of Natural Science – Citadel, Victoria.
5. Ġgantija Temples – Xagħra.
6. Xagħra Stone Circle – Xagħra.
7. Ta' Kola Windmill – Xagħra.

Appendices

Appendix C – COBIT Controls

COBIT defines IT activities in a generic process model within four domains.[4] These domains are Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate as depicted in Figure 6. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

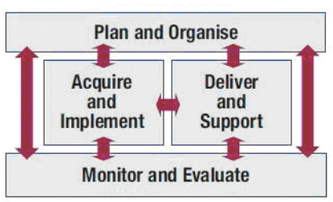


Figure 6

Plan and Organize

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 realized from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource 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.

[1] COBIT 4.1 Framework - http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

Appendix C – Cont.

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, analyzed and assessed. Risk mitigation strategies are adopted to minimize residual risk to an accepted level. 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 realize 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

Appendices

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. This process 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 minimizes 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, utilizing offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimizes 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 minimize 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.

Appendices

Appendix D – Fire Suppression Systems[5]

The fire suppression system is used in conjunction with smoke detectors and fire alarm systems. The medium for fire suppression varies, but is usually one of the following:

- Water-based systems are typically referred to as sprinkler systems. Even if these systems are effective they are also unpopular because they damage the equipment present in the room.

- Dry-pipe sprinkling systems do not have water in the pipes until an electronic fire alarm activates the water pumps to send water in the system. Dry-pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment from above.

- FM-200 is a colourless odourless gaseous halocarbon. It is commonly used as gaseous fire suppression agent. This agent suppresses fire by discharging as a gas onto the surface of combusting materials. Large amounts of heat energy are absorbed from the surface of the burning material, lowering its temperature below the ignition point.

Apart from the above, there are other medium of fire suppression systems, however, Carbon Dioxide (CO2), Argonite and Halon systems are dangerous as they are unable to sustain human life when pressurised gas is released into the area to replace the oxygen for combustion.

[5] Information on Fire Suppression Systems as per www.isaca.org

Appendix E – Restrictions on use of E-mail and Internet services[6]

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 in 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 (25) e-mail users, if such unsolicited e-mailing provoke 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.

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

Appendices

Appendix E – Cont.

Restrictions on use of Internet services

Similiarly, every user should abide by the restrictions on use of the 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 (10) 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.

Appendix F – Business Continuity and Disaster Recovery Plan[7]

A Business Continuity Plan should:

- Be consistent with Heritage Malta's overall mission, strategic goals and objectives.
- Be documented and written in simple language and understandable to all.
- Provide management with an understanding on the adverse effects on Heritage Malta, resulting from normal systems or service disruption and the total effort required to develop and maintain an effective BCP.
- Identify the information assets related to core business processes.
- Assess each business process to determine its criticality.
- Validate the RPO and the RTO for various systems and their conformance to Heritage Malta's objectives.
- 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 the conditions that will activate the contingency plan.
- Identify which resources will be available in a contingency stage and the order in which they will be recovered.
- Identify the key persons responsible for each function in the plan.

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

Appendices

Appendix F – Cont.

- Identify the methods of communication among the key persons, support staff and employees.
- 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 Heritage Malta on the effect this might have on Heritage Malta in the event of a disaster.

A Disaster Recovery Plan should contain the following information:

- A statement detailing the scope and capability of the disaster recovery plan, exactly when should this plan be used and what is the impact on Heritage Malta.
- A description of the key roles and responsibilities so that anyone assigned to a particular role in the recovery team understand what is required of them.
- 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 by Heritage Malta.
- Detailed recovery activities and sequence of events, including pre-requisites, dependencies and responsibilities.