NAO
National Audit Office
MALTA

Information Technology Audit

Commerce Department

Report by the Auditor General

January 2015

Information Technology Audit

Commerce Department

Table of Contents

List of Tables

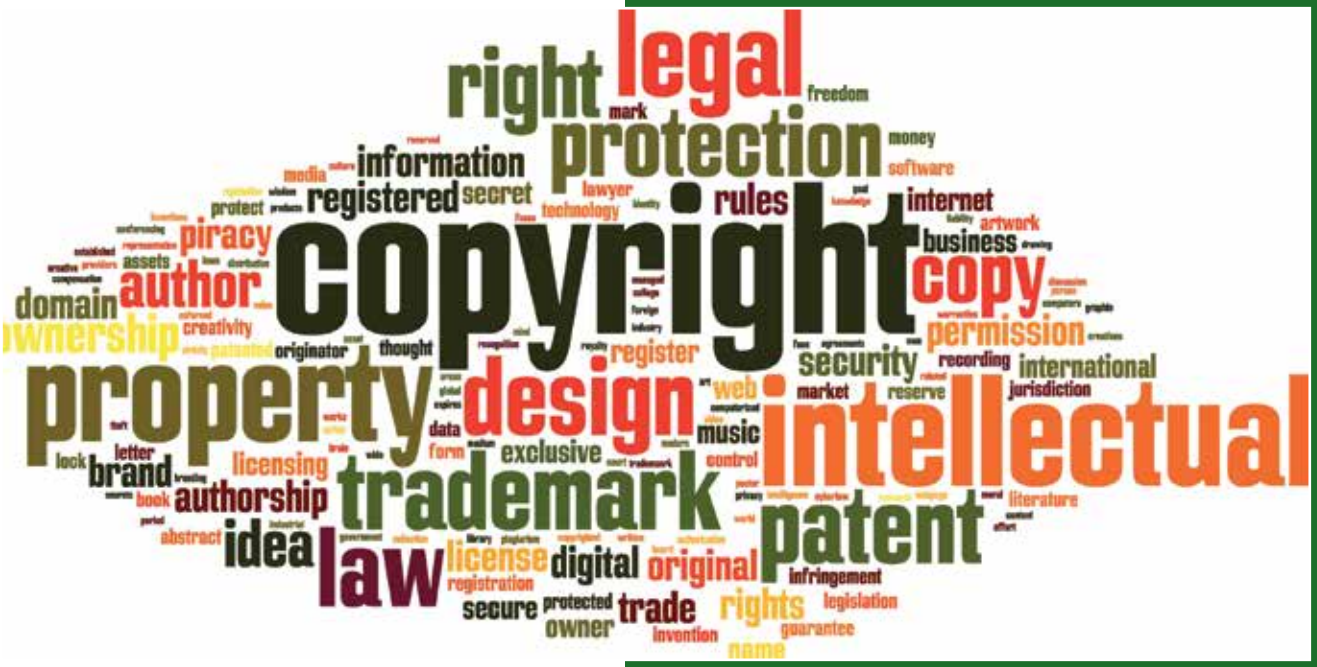
List of Figures

List of Abbreviations

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

AD	Active Directory
ADSL	Asynchronous Digital Subscriber Line
AMS	Absence Management System
BCP	Business Continuity Plan
CCTV	Closed-Circuit Television
CdB	Common Database
CDRT	Centre for Development, Research and Training
CIMU	Central Information Management Unit
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
CMS	Content Management Systems
DAS	Departmental Accounting System
DCS	Director of Corporate Services
DOCREG	Document Registry
DoS	Denial of Service
DRP	Disaster Recovery Plan
DUeS	Dual Use e-System
e-Forms	Electronic Forms
e-mail	Electronic Mail
eRFS	Electronic Request for Service
ETC	Employment and Training Corporation
EU	European Union
FMMU	Financial Management Monitoring Unit
FMS	Fleet Management System
FSS	Final Settlement System
GMICT	Government of Malta Information and Communication Technology
HR	Human Resources
ICT	Information and Communications Technology
IPRD	Industrial Property Registrations Directorate
IMI	Internal Market Information
IMU	Information Management Unit
IP	Intellectual Property
IT	Information Technology
ITSM	IT Service Management
LAN	Local Area Network
LMS	License Management System
LPO	Local Purchase Order
MAGNET	Malta Government Network
MEIB	Ministry for the Economy, Investment and Small Business

MEPA	Malta Environment and Planning Authority
MFSA	Malta Financial Services Authority
MITA	Malta Information Technology Agency
MITC	Ministry for Infrastructure, Transport and Communications
NAO	National Audit Office
NESA	National Enterprise Support Award
NSO	National Statistics Office
OA	Office Automation
OHIM	Office for Harmonisation of the European Internal Market
OPM	Office of the Prime Minister
PAHRO	Public Administration Human Resources Office
PC	Personal Computer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIGL	Système Intègrè de Gestion de Licenses
SLA	Service Level Agreement
SME	Small and Medium-sized Enterprises
TM	Trademark
TMS	Trademark System
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
VRT	Vehicle Roadworthiness Test
WAIS	Wassenaar Arrangement Information System
WAN	Wide Area Network



Executive Summary

Executive Summary

Background

The National Audit Office (NAO) carried out an Information Technology (IT) audit within the Commerce Department. This audit sought to examine the Department's IT operations and related investments to ensure that IT is successful in delivering the business requirements.

The aim of this report is to collect and analyse evidence to determine whether the Commerce Department has the necessary controls in place to ensure that their IT and Information Systems maintain data integrity, safeguard assets, allow organisational goals to be achieved effectively and assist in making efficient use of the Government IT relates resources. This IT audit report therefore identifies the potential risks and makes the necessary recommendations to mitigate those risks.

Key Findings and Recommendations

The key issues addressed in this report (Chapter 2 refers) focused on how the Commerce Department is managing its Information and Communications Technology (ICT) resources, in terms of hardware and software applications, network infrastructure and supplier management. The main findings and corresponding recommendations are listed below:

a. The Commerce Department does not have a formally documented IT strategy plan;

b. The NAO remarked on the high usage of local printers and their related running costs. In this regard, the NAO was informed that the Commerce Department intends to adopt a greener environment by reducing the amount of local printers installed and instead introduce a networked multi-function printer in every Directorate;

c. The NAO commends the initiative that was taken by the Ministry's Information Management Unit (IMU) in publishing a Printing Policy and distributing it across all the Departments within the Ministry for the Economy, Investment and Small Business (MEIB), with the aim to ensure the efficient use of printing resources and reduce the associated running costs;

d. Whilst the IT Unit and the Ministry's IMU keep track of the Commerce Department's IT hardware inventory in separate spreadsheets, the NAO recommends that the Ministry's IMU carries out an internal audit to verify that all the Personal Computers (PCs) and laptops are compliant in terms of authenticity of software applications and software licenses. As a result of this audit, the Ministry's IMU should compile an inventory list of all software applications in use and their respective licences, and amalgamate this list with the hardware inventory list;

e. The NAO noted that one of the third party supplier's services and maintenance contract was not updated and still refers to the previous owner under the then Ministry for Infrastructure, Transport and Communications (MITC). In this regard, the NAO recommends that the Commerce Department should ensure that all the third party supplier's services and maintenance contracts are duly updated to reflect any changes and if necessary, a covering letter should be signed by both parties and attached to the respective contract.

The IT audit reviewed seven software applications used within the Commerce Department (Chapter 3 refers) in terms of ease-of-use, security controls, account management and hosting services. The main findings and corresponding recommendations are listed below:

a. The NAO was informed that all the vacation leave cards prior to 2014, of every individual within the Commerce Department, have to be inputted manually into the Dakar Absenses Management System (AMS) module. Unfortunately, due to the lack of resources, at the time of this IT audit, this process is being carried out after office hours, but to date the Department cannot quantify the effort required to input all the data. In this regard, the NAO recommends that the Commerce Department should establish a cut-off date, analyse the amount of vacation leave cards that needs to be processed and the effort required to input all the data, taking into consideration the resources available;

b. The NAO observed that even though the Commerce Department makes use of two service stations, one of the service stations is listed twice in the Fleet Management System (FMS) but under a different heading. Even though the Commerce Department is aware of this, the NAO recommends that the Department should liaise with the Financial Management Monitoring Unit (FMMU) within the Ministry for Finance and rectify this problem by grouping all the data under one service station heading;

c. The NAO was informed that the current FMS software application is currently in the process of being migrated from a client server application to a web solution referred to as the Fleet Web Portal;

d. Whilst reviewing the License Management System (LMS), the NAO observed that in 2013, 1,944 Trade Licences were issued when compared to 1,188 in 2012;

e. The Stock Ledger software application was developed as an "interim application" to the new Corporate Finance Management Solution, which is planned to be implemented by 2016;

f. The NAO observed that between July 2013 and July 2014, the total number of applications received for the registration of trademarks amounted to 880, whilst the total number of trademarks registered within that period amounted to 999;

g. The current Trademark System (TMS) will soon be replaced by a modern Back Office application, which will be provided by the Office for Harmonisation of the European Internal Market (OHIM). The new system will be implemented in two stages and should be running live in mid-December 2014;

h. At the time of this IT audit, the total number of trademarks found in the TMview web application amounted to 24,477,698. These are attributed to the number of trademarks provided by all the participating offices, of which 52,062 are provided by the Commerce Department.

This audit report also reviewed the key components and the extent of Information Security measures (Chapter 4 refers) and whether the Commerce Department adheres to Government security policies and procedures to maintain the confidentiality, integrity and availability of data.

a. The NAO commends the initiative taken by the Ministry's IMU in providing the Department's IT Unit with a data wiping software application to ensure that confidential information is securely erased from Hard disks whenever a PC or laptop is transferred to another user or disposed of;

b. The NAO recommends that a policy should be drafted and communicated internally describing the procedure to be adopted for the disposal of any confidential information that may reside on paper, flash memory devices, CD/DVDs either through shredding, secure wiping and/or physical destruction etc;

c. The NAO recommends that Information Security Awareness guidelines and training should be ongoing, whereby officials within the Commerce Department are provided with regular updates to foster security awareness and compliance with security policies and procedures.

The final component of the report (Chapter 5 refers) delved into the management and controls of IT operations:

a. Overall, the Commerce Department lacks in physical access controls. In this regard, the NAO was informed that discussions are currently underway with the Commerce Department and the Ministry's IMU, on how to enhance the physical access controls within the building;

b. The Department should market the use of electronic-Forms (e-Forms), since they are hardly being used. The NAO recommends that the Commerce Department reviews the current e-Forms and ensures that they are all updated and accompanied with a proper workflow, especially in view of a possible increase in e-Forms usage as a result of a wider distribution of e-ID in the coming months;

c. The NAO observed that offline mailboxes of personal or generic e-mail accounts are being stored locally on the end user's PC or laptop. In this regard, the NAO recommends that the Ministry's

IMU together with the Department's IT Unit should provide guidelines to all the officials within the Department, on how to backup and securely store offline mailboxes;

d. Even though all the IT systems are hosted at MITA-01 Data Centre in St. Venera, the Commerce Department does not have a formalised Business Continuity Plan (BCP) and Disaster Recovery Plans (DRP) at the Department level;

e. The NAO recommends that the Commerce Department should perform a Business Impact Analysis and a Risk Assessment exercise from which a BCP and a DRP can be drafted at the Department level.

The final Chapter of this report lists the Management comments submitted by the Commerce Department.

Chapter 1

Introduction

Chapter 1

Introduction

1.1 Overview

The Commerce Department was set up towards the end of 2000, on the recommendation of the Operations Review that was carried out by the then Ministry for Economic Services. The aim of the Commerce Department is:

"To assist business and facilitate trade whilst providing the necessary infrastructure to encourage the securing, utilisation and respect of intellectual property rights"

This audit report, issued by the IT Audits and Operations Unit within the NAO, documents the current state of IT operations within the Commerce Department. All the findings and recommendations that resulted from this risk based IT audit, are included in this report.

1.2 Organisation Structure

The Commerce Department is located at Lascaris Bastions in Valletta, and is composed of the Industrial Property Registrations Directorate (IPRD), the Trade Services Directorate and the Small Business and Crafts Directorate assisted ably by its Support Services arm. The organisation chart in Appendix A depicts how the Commerce Department is set up.

The IPRD – this Directorate is responsible for the registrations of Industrial Property, namely trademarks, patents and designs, as well as the broader Copyright Policy forming the Intellectual Property Affairs that it oversees, under the direct authority of the Comptroller of Industrial Property, who is also the Commerce Department's Director General.

The IPRD is responsible for the registration of trademarks in accordance with the Trade Marks Act of 2000 as well as the registration of designs and patenting of inventions in conformity with the Patents and Designs Act of 2000. This Directorate is also involved in the updating and upgrading of the legislation on Copyright.

Thus, the IPRD receives, analyses and processes applications for the registration of trademarks, industrial designs and patents. It also performs other tasks in connection with these applications and registrations, such as the recording of assignments, renewals, and other changes which may occur. In this way, the registers, which are also available for public inspection, show the status of the trademarks, designs or patents concerned.

The Trade Services Directorate – this Directorate is made up of the Import/Export Licensing Unit and the Trade Licensing Unit. These commercial activities may be personal to an individual (example: Street and Market Hawkers, Buskers or freelance activities) or to premises, which carry out a commercial activity from such premises.

Although many import licences have been removed, there are a number of items that need an import or export licence such as military equipment and goods of a dual-use nature, together with imports coming from countries outside the European Union (EU).

The Small Business and Crafts Directorate – this Directorate facilitates the interaction between Entrepreneurs and any Authority, Body, Ministry or Department, which renders a service to small business. It gathers all the relevant information to pass it on to those concerned with helping small businesses flourish and to assist in the process, which leads to an improved and simplified business environment.

Furthermore, the Directorate also gives administrative support to the Malta Crafts Council, operates the Malta SOLVIT Centre and facilitates the implementation of the Internal Market Information[1] (IMI) system. The Directorate also provides secretariat to the Malta Crafts Council. The latter was established under the Act XXI of 2000, which provides for the encouragement, promotion and regulation of crafts and craftsmen.

At the time of this IT audit, the Commerce Department had a staff compliment of 67 personnel as depicted in Table one below. To-date, the Commerce Department offers flexible work arrangements to its employees, whereby 14 employees are offered teleworking, three employees work on a reduced timetable whilst 39 employees work on a flexible work schedule.

Commerce Department	Male	Female
Director General's Office	1	4
Industrial Property Registration Directorate	6	11
Trade Services Directorate	8	8
Small Business & Crafts Directorate	2	3
Business Care Unit	0	4
Support Services	11	9
Total Staff Compliment	**28**	**39**

Table 1 - Staff Compliment

[1] http://ec.europa.eu/internal_market/imi-net/index_en.htm

1.3 Legislation

For the performance of its functions, the Commerce Department refers mainly, but not exclusively to the following legislations:

- Chapter 421 Malta Crafts Council Act;
- Subsidiary Legislation 421.01 Registration of Craftsmen and Entrepreneurs (Malta Crafts Council) Regulations;
- Subsidiary Legislation 421.02 Maltese Craft (Constitution) Order;
- Chapter 417 Patents and Designs Act, 2000 and regulations;
- Chapter 415 Copyright Act and regulations;
- Chapter 416 Trademarks Act and regulations;
- Chapter 441 Trading Licences Act and regulations;
- Subsidiary Legislation 117.02 Exportation Control Regulations;
- Subsidiary Legislation 117.14 Importation Control Regulations;
- Subsidiary Legislation 365.12 The Dual Use Items (Export Control) Regulations;
- Subsidiary Legislation 365.13 The Military Equipment (Export Control) Regulations.

1.4 ICT within the Commerce Department

Apart from the Office Automation (OA) software applications, the Commerce Department makes use of a number of IT software applications, which include amongst others:

- **Common Database (CdB)** – It is a central data repository used by authorised persons within the Government Departments to access information about persons, addresses, organisations and the inter-relationships between these subjects found in the Public Domain;
- **Dakar** – It provides payroll processing of all the employees. This includes the maintenance of the Department's employee details, the management of leave, actual payroll calculation, printing of payroll reports and payslips, processing of direct credit payments and submission of periodical Final Settlement System (FSS) returns as required by the current legislation;
- **Departmental Accounting System (DAS)** – It is the main accounting system in use to record and control revenue and expenditure across all Government Departments;

- **Document Registry System (DOCREG)** – This system is used by the Registry Section within the Commerce Department, to acknowledge and track files and correspondence through the system;

- **Dual Use e-System (DUeS)** – It is a web-based application, which is mainly used for information sharing between EU Member States on dual use of goods;

- **e-Bridge** – This is a third party web application which is used to maintain and update the Malta Crafts Portal[2];

- **Fleet Management System** – It is the main source of management and control of all the vehicles to suit the needs of the various Ministries and Departments;

- **Internal Market Information System** – This system, which was developed by the European Commission, is a secure online tool used between Member State authorities and the European Commission. It facilitates the exchange of information between competent authorities by enabling them to easily find their counterparts in other Member States and to communicate with them quickly and efficiently. It helps overcome practical barriers to communication, most importantly differences in administrative structures, languages and a lack of clearly identifiable partners in other Member States;

- **License Management System** – This system is used to manage Trade Licences, monitor their activity, payments history, reporting and to meet a variety of other business needs;

- **Malta Financial Services Authority (MFSA)** – This is a third party web application whereby authorised officials within the Commerce Department can download official documents against a minimal charge per document. This web application is accessed amongst others to check whether a particular company is in dissolution, to check whether a particular company is struck off, amalgamated or defunct, to confirm or otherwise the list of directors, and to obtain the respective addresses;

- **Soprano** – This application is used to record Maltese patents, issue certificates or grants and to send correspondence or renewal notices. The NAO was informed that this application is currently not being used and will be replaced by a different application in the near future;

- **Stock Ledger** – This application is used for storing data regarding purchases made by the Department and to keep a detailed record of what is being spent. Detailed reports are sent every quarter to the Treasury Department, within the Ministry for Finance, in order to be accountable of the spending done by the Procurement Unit within the Commerce Department;

- **Système Intègrè de Gestion de Licenses (SIGL)[3]** – It is a web application tool developed within the EU Member States for the management of licenses for imports of textiles, clothing, footwear, steel and wood to the EU;

[2] https://secure3.gov.mt/maltacrafts/

[3] http://trade.ec.europa.eu/sigl/

- **Trademark System** – This application is used solely by the Commerce Department for the registration of new trademarks and designs and for the patenting of new inventions. The system is also used for the renewal of existing trademarks, designs and national patents as well as to carry out industrial property searches;

- **Trademark (TM) view** – This is an online consultation tool allowing any Internet user to search, free of charge, the trademarks of all participating official trademark Offices. It thus offers a multilingual and gives access to trademark applications and registrations of the participating official trademark offices.

For the purpose of this IT audit, the NAO has evaluated the seven major applications listed below:

- Dakar;
- e-Bridge;
- Fleet Management System;
- License Management System;
- Stock Ledger;
- Trademark System; and
- TMview.

The NAO also reviewed the management and maintenance of the Commerce Department's website, the two current Facebook pages, the Commerce Department's e-Forms and the ICT Infrastructure, which consist of:

- **PCs and laptops** – The PCs and laptops are acquired through the IMU within the MEIB. At the time of this IT audit, the Commerce Department had 47 PCs and 13 Laptops;

- **Network** – The Commerce Department is connected to the Malta Government Network (MAGNET) through a fibre-optic connection;

- **ADSL Connection** – The Commerce Department has a third party Asynchronous Digital Subscriber Line (ADSL) with a local service provider and is only used for video conferences purposes;

- **Electronic mail (e-mail) system** – The Commerce Department utilises the Government's e-mail system;

- **OA software applications** – All the Microsoft software licences are acquired through the Malta Information Technology Agency (MITA) under the Government Enterprise Agreement and the respective licenses are managed by the IMU within the MEIB.

1.5 Audit Scope and Objectives

The aim of this IT audit is to collect and analyse evidence to determine whether the Commerce Department 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 the Government IT related resources. This report includes the recommendations made by the 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 the Commerce Department's Director General, to gather the necessary information on the audit site prior to undertaking an on-site audit. The aim of the questionnaire was to familiarise the audit team with the Commerce Department and its IT setup prior to the audit visit;

- The Commerce Department's overall strategic direction, objectives, internal structures, functions and processes were then studied in order to gain a comprehensive understanding of the Department and its environment. This included in-depth interviews with key officials and stakeholders, as well as observations, reviews of 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, and for any BCP and DRP that exist.

Thus, the objective of this report was to:

- Analyse all the information collected during the course of the IT audit;

- Verify whether the IT applications utilised are being used efficiently and effectively;

- List all the findings and identify any potential risks;

- List all the recommendation to mitigate those risks.

1.6 Audit Methodology

To achieve these objectives, a number of interviews were held with a number of stakeholders within the Commerce Department. Furthermore, a walkthrough was held at the Commerce Department to familiarise with the procedures of the different applications being used and the overall IT setup within the Department.

The audit report also refers to the Control Objectives for Information and related Technology (COBIT) set of best practices, which are listed in Appendix B. COBIT, is a comprehensive set of resources that contains all the information organisations need to adopt 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.

1.7 Structure of the Report

The report comprises five further Chapters, each documenting the information collected and highlighting the findings and recommendations:

- Chapter 2 covers the IT governance and management by evaluating the manner in which ICT resources are managed;

- Chapter 3 reviews a selection of IT applications that are currently being used within the Commerce Department;

- Chapter 4 addresses the key components of information security and evaluates the security measures implemented within the Commerce Department, to maintain the confidentiality, integrity and availability of data;

- Chapter 5 analyses whether the Commerce Department is managing and controlling its IT operations in the most effective way. Furthermore, it addresses whether the Department is confident with any BCP or DRP in the event of a service disruption;

- Chapter 6 lists all the management comments submitted by the Commerce Department.

1.8 Acknowledgement

The NAO would like to express its thanks and appreciation to the Ministry's Chief Information Officer (CIO) and all the officials within the Commerce Department, who were involved in this audit in particular the Director General, Directors, Assistant Director Support Services and the Senior System Administrator, for their time, patience and assistance.

Chapter 2

IT Management

Chapter 2

IT Management

2.1 IT Unit

The Commerce Department has a Senior System Administrator, who was appointed on 1st November 2013 to manage the IT Unit. The latter, which is made up of a Senior System Administrator only, reports directly to the Assistant Director Support Services within the Commerce Department and to the Ministry's CIO.

The main functions of this IT Unit are:

- To control and manage all the ICT services;
- To co-ordinate, supervise and manage IT projects; and
- To keep an updated inventory of all the ICT assets within the Department.

The NAO observed that there is a very good level of communication between the Commerce Department's Director General and the IT Unit, whereby meetings are held every fortnight to provide the necessary updates of any projects or issues that are being tackled by this Unit. The same level of communication exists between the IT Unit and the Ministry's CIO, MITA and the respective third party suppliers.

The NAO was informed that the IT Unit, together with the Ministry's CIO, are currently working on the development of a new website to replace the existing Department's official website. In this regard, the NAO was informed that the Department's new website should be launched by the end of February 2015.

2.2 IT Strategy

An IT strategy is typically a long-term action plan for achieving a goal, set in the context of a rapidly changing technology environment. It covers all facets of technology management, including cost management, human capital management, hardware and software management, vendor management, risk management and all other considerations one can find in an IT environment.

Many organisations choose to formalise their IT strategy in a written document or balanced scorecard strategy map. The plan and its documentation should be flexible enough to change in response to new organisational circumstances and business priorities, budgetary constraints, available skill sets and core competencies, new technologies and a growing understanding of user needs and business objectives.

The NAO was informed that the Commerce Department does not have a formally documented IT strategy plan or refer to a specific IT strategy. However, the Commerce Department together with the Ministry's IMU have a formalised plan documenting the proposed IT projects for the forthcoming year. In this regard, the NAO recommends that the Commerce Department formulates an IT strategy that should focus on creating and measuring the business value from the investment in ICT.

2.3 ICT Expenses

The NAO noted that the ICT budgetary expenditure is planned as part of the budgetary projection exercise, which is carried out on a yearly basis, by examining the expenditure incurred during the previous year, taking into consideration any initiatives or projects to be implemented in the coming year and any inflationary increases. These projections are then submitted to the Budget Office, within the Ministry for Finance, for onward forwarding to the Budget Office. In this regard, the ICT Budget for 2014 was set up by the Ministry's IMU following several discussions between the Ministry's CIO, the Commerce Department's Director General, the Directors of each Directorate and other key officials within the Department. The ICT Budget is thus formalised after taking into consideration any projects that are to be implemented by the respective Directorates that require ICT support or investment, whether the current IT systems need to be replaced or enhanced, any anticipated requests for teleworking and if new ICT peripherals, office communications and other ICT equipment are required.

During the course of this IT audit, the NAO reviewed the actual ICT capital and recurrent expenses of the Commerce Department in 2013 and that planned for 2014.

ICT Expenses	Total Operational and Capital Expenditure
2013 (Actual)	€102,296.39
2014 (Planned)	€159,406.00

Table 2 - Commerce Department ICT Expenses

As depicted in Table two, the Total Operational and Capital Expenditure for 2013 amounted to €102,296.39, which includes €77,066.61 on Capital Expenditure and €25,229.78 on Operational Expenditure. On the other hand, the planned ICT Capital and Operational Expenditure for 2014 amounted to €159,406.00, of which €10,106 is planned for ICT Operational Expenditure related to the maintenance of the Commerce Department's Intellectual Property (IP) Portal and Crafts Portal (€5,428), a new Commerce Department Portal (€2,200) and the remaining (€2,478) on hardware maintenance agreements. Furthermore, €149,300 is planned for ICT Operational Expenditure, namely

the costs incurred in the running of the Commerce Department e-Forms (€50,600), the replacement of local printers with multi-function printers (€49,000) and the remaining capital allocated to any other expenses incurred by the Commerce Department (€49,700). This entails an increase of €57,109.61 on the total amount from the previous year.

Whilst going through the ICT Capital Expenditure for 2013, the NAO noted that the main expenses were related to the setup of a new Data Communication line (€43,272.96) and to the external costs incurred for the development of the TMview software application (€27,600). On the other hand, the NAO noted that out of €25,229.78 incurred on Operational expenses, €18,241.13 were related to toner costs due to a high number of local printers installed on most of the PCs and laptops. In this regard, the NAO remarked on the high usage of local printers and their related running costs. In return, the NAO was informed that the Commerce Department intends to adopt a greener environment by reducing the amount of local printers installed and will instead introduce a networked multi-function printer in every Directorate. During the course of this IT audit, the NAO was informed that in September 2014, a Printing Policy was published by the Ministry's IMU and distributed to all the Departments within the MEIB with the aim to:

- Reduce the associated costs, as well as optimising value for money;
- Maximise efficiency and minimise environmental impact; and
- Provide management with the necessary information to map trends of usage and plan for future requirements.

The NAO commends this initiative and to achieve the above objectives, the Commerce Department must ensure that everyone abides by this policy for the efficient use of resources. In the meantime, the NAO recommends that as best practice, the Commerce Department together with the Ministry's IMU implement a cost-benefit analysis of the Department's ICT infrastructure related expenditure and investments, with the aim:

- To determine if a project, decision or government policy offers a sound investment/decision; and
- To provide a basis for comparing the total expected cost of each option against the total expected benefits, to see whether the benefits outweigh the costs and by how much.

2.4 Systems Development Life Cycle

During the course of this IT audit, the NAO reviewed the IT systems development life cycle adopted by the Commerce Department in terms of the processes involved in the procurement, maintenance and disposal of ICT hardware equipment and the planning, development, acquisition, testing, implementation and maintenance of software applications within the Commerce Department.

2.4.1 Hardware Asset Management

Hardware asset management comprises the management of the physical components of computers and computer networks, from acquisition through disposal. Common business practices include the request and approval process, procurement management, life cycle management, redeployment and disposal management.

2.4.1.1 Procurement

Over the past years, Government has leased PCs and laptops from two contractors following public procurement. When the PC leasing arrangement was introduced, Government replaced its ageing PC population in bulk and achieved its standardisation objective. The leasing agreement included the provision of workstations support.

After five years, this support contract expired, and the hardware support on workstations on most workstations expired as well. In this regard, the Government identified the best way forward to ensure that the procurement of hardware and the provision of hardware and software support is achieved in an efficient and effective way.

To trigger the procurement process, the NAO was informed that the IT Unit and Senior Management within the Commerce Department will liaise with the Ministry's IMU. If sufficient funds are available for the procurement of any PCs or laptops, the IMU would send a business case by e-mail to the MITA Software Licensing Management to approve the necessary licences. MITA will then issue a quotation to the IMU, who in return will issue a Local Purchase Order (LPO) and sends it by e-mail or post to MITA. Upon receipt of the LPO, MITA will then place the order on behalf of the Department with the respective supplier. The latter will then deliver the PCs or laptops at the Commerce Department within the established Service Level Agreement (SLA). The IT Unit will then acknowledge the delivery and commissioning of the PCs or laptops by signing the delivery note. The supplier will then send the signed delivery note by e-mail to MITA's Procurement Section. In return, MITA will then update the Procurement records with the hardware details accordingly and will finally issue an invoice to the Commerce Department to effect payment.

If the Commerce Department intends to procure other IT equipment, such as multi-function printers, the IT Unit will liaise with the Ministry's IMU to ensure whether sufficient funds are available. The IT Unit will then define the specifications of the required hardware, obtain the necessary approvals from senior management and the Ministry's IMU and acquire the hardware needed in line with the Government procurement regulations.

2.4.1.2 Maintenance

A hardware repair can be broadly defined as a support intervention that requires hardware to be changed or that requires the hardware to be serviced or repaired. In this regard, the respective supplier, within the Government procurement process, carries out any hardware repairs for PCs or laptops procured through the Government procurement process.

During the course of this IT audit, the NAO observed that the IT Unit, within the Commerce Department, is the point of contact between the end user and MITA. Thus, in the event of a hardware or software malfunction, the IT Unit would raise a service request with MITA's Service Call Centre. If the problem could not be resolved over the phone, the service request is escalated to the respective Workstation Support Contractor. Service requests that are initially serviced by the Workstation Support Contractor, which are diagnosed to require hardware repair/or replacement, are escalated to the respective supplier within the Government procurement process.

The NAO noted that these repairs are performed by the respective supplier within the corresponding SLA, as defined in the Government procurement process. If following the hardware repair, the PC or laptop requires a software re-imaging, this is carried out as part of the hardware repair process. In such instances, the PC or laptop will have to be commissioned again as part of the repair process. This entails the transfer of any data (such as offline mail or secure mail certificates) onto the new image or workstations from backup media, rename the PC or laptop and "join" it to the Domain.

On the other hand, if the PC or laptop is taken from the end user for repairs, the supplier might be required to commission a temporary PC or laptop in order to allow the end user to continue working, especially if the necessary spare part to fix hardware problems of a PC or laptop is not available. The temporary replacement is expected to have equivalent or better specifications than the PC or laptop being replaced but not necessarily of the same brand. A target date by when the original machine is returned to the end user must be agreed upon and documented.

During the course of this IT audit, the NAO observed that whenever a service request is raised with MITA's Service Call Centre, all the e-mail correspondence with MITA is stored in an offline mailbox, whilst the Supplier's job chit is kept by the end user or handed in to the Commerce Department's IT Unit. A similar procedure applies for any repairs or maintenance of printers or other IT equipment. However, the NAO observed that since all the e-mail correspondence is stored in an offline mailbox, the IT Unit is not in a position to easily identify or analyse trends and calls of a particular nature, which collectively may indicate a common source. In this regard, the NAO suggests that the IT Unit should at least keep tabs of IT requests of a hardware nature and record them electronically.

2.4.1.3 Disposal

During the course of this IT audit, the NAO reviewed how the Commerce Department disposes of IT equipment that is either obsolete or beyond economical repair. The NAO was informed that from time to time, the Commerce Department appoints a board to decide which IT equipment is to be disposed of and to ensure that this is carried out accordingly.

In this regard, the NAO was informed that the Commerce Department has recently gone through this process, whereby a board specifically appointed by the Director Corporate Services (DCS) within the MEIB, determines whether a number of IT equipment is obsolete or beyond repair. Following a decision taken by the board, a statement or report of the final list of IT equipment to be disposed of is handed in to the IT Unit. The latter will then update the IT inventory database before handing over the list to the Assistant Director Support Services for file keeping.

In the meantime, the NAO is pleased to note that if a PC or laptop is to be disposed of, the IT Unit ensures that there is no data residing on the Hard disk. In this regard, the NAO was informed that the IT Unit adopts the Government of Malta Information and Communication Technology's Desktop Services Procedure (GMICT R 0084:2009)[4] in terms of PC disposal and data wiping to ensure that any data residing on the equipment to be disposed of would not be retrieved by any third party.

2.4.2 Software Asset Management

During the course of this IT audit, the NAO reviewed the project life cycle in terms of software asset management. The latter is a business practice that involves managing and optimizing the purchase, deployment, maintenance, utilization and disposal of software applications within an organisation.

When adopting a project life cycle approach, one has to take into consideration the six phases listed below:

- **Feasibility/Requirements study phase** – The feasibility and requirements of the desired software is determined in this phase;
- **Design phase** – Producing a conceptual design that meets the requirements;
- **Development phase** – Developing code for be-spoke software or choosing an off-the-shelf package that meets the requirements;
- **Testing phase** – Verifying that the software works and meets the requirements;
- **Implementation phase** – Implementing the software application;
- **Maintenance phase** – Maintaining the software application throughout its lifetime.

The NAO has thus reviewed the project life cycle approach in terms of planning, development, testing, implementation and maintenance. In this regard, the NAO was informed that the contracted third party suppliers, following internal discussion with the Commerce Department, carry out the majority of the software project life cycle.

However, the NAO recommends that the Commerce Department should ensure that the software project life cycle is adopted when procuring a new software application or when new enhancements to existing software applications are made. In this regard, the NAO was provided with a number of documented manuals, which include amongst others implementation plans, software architecture designs, test plans and support maintenance plans, which were compiled by the respective third party suppliers. The NAO commends these documented manuals and is pleased to note that the third party suppliers adhere to change management procedures whenever any changes or enhancements are required to the system.

[4] Desktop Services Procedure - https://www.mita.gov.mt/MediaCenter/PDFs/1_GMICT_R_0084_Desktop_Services.pdf

2.5 IT Inventories

An IT inventory gathers detailed hardware and software inventory information, which is then used to make decisions about hardware and software purchases and redistribution.

The NAO noted that the IT Unit has an updated hardware inventory, which is continuously being updated on a spreadsheet. As depicted in Figure one, at the time of this IT audit, the IT Unit is responsible for the Video Conferencing equipment, three Photocopiers, 56 LCD/TFT Monitors, two Projectors, five Scanners, seven All-in-one Printers, 41 Stand-alone Printers, 13 Laptops and 47 PCs.

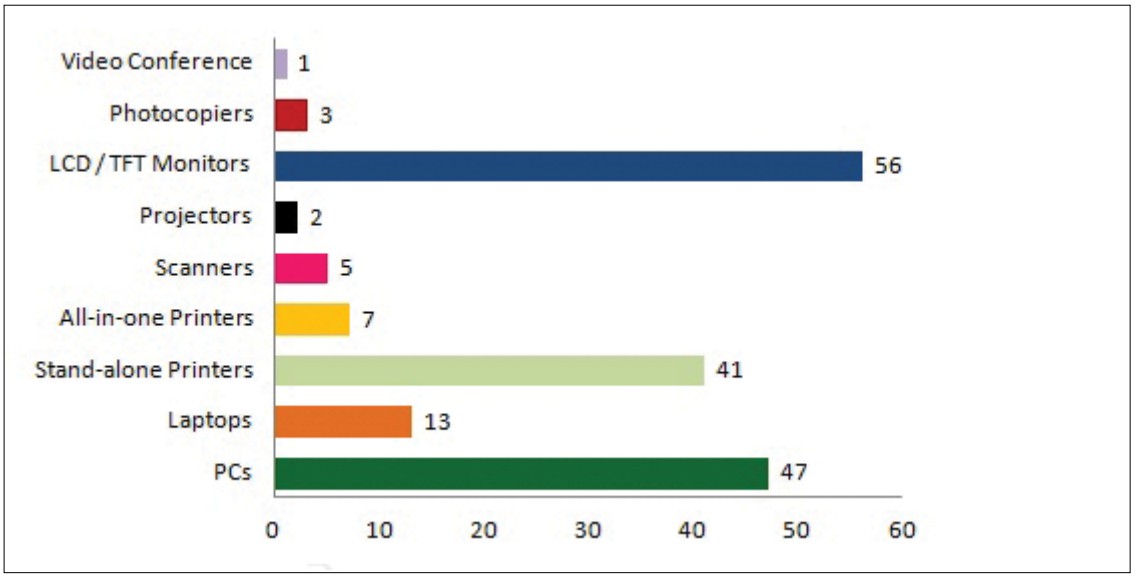


Figure 1- Hardware Inventory

During the course of this IT audit, the NAO was informed that the Ministry's IMU carried out an IT inventory whereby every piece of IT equipment within the Commerce Department was affixed with an inventory sticker provided by the Ministry's IMU. In this regard, the IT Unit took this opportunity to crosscheck the data within the IT Unit's hardware inventory spreadsheet with the Ministry's IMU inventory sheet to ensure that every IT component is in place. In the meantime, the NAO was informed that the IT Unit intends to carry out an inventory exercise on the Commerce Department's LAN infrastructure to ensure that only the network points that are in use are held active.

With reference to the software inventory, the NAO was informed that this list is currently being maintained by the Ministry's IMU. In this regard, the NAO recommends that the Ministry's IMU carries out an internal audit to verify that all the PCs and laptops are compliant in terms of authenticity of software applications and software licences. As a result of this audit, the Ministry's IMU should compile an inventory list of all software applications in use and their respective licenses and amalgamate this list with the hardware inventory list.

2.6 Third Party Suppliers

To conform to the Office of the Prime Minister (OPM) Circular No. 29/2005, MITA being the ICT Agency for the Government of Malta, was entrusted with the provision of ICT core services to all Government and Public Sector Entities.

In this regard, MITA provides the Commerce Department with a fibre-optic connection to the Government Network, generally referred to as MAGNET, and provides 24x7 monitoring to this connection, namely on the core Wide Area Network (WAN) equipment and core access switches, to prevent potential ICT problems resulting in service downtime. Furthermore, MITA is also providing the Commerce Department with a number of other services:

- E-mail;
- Internet browsing and filtering;
- Standard Desktop Security Configuration Services, such as Anti-virus, patch management and spam filtering of e-mails via black lists and tagging;
- Hosting of Server services and any Guest Virtualised Machine in a segregated environment within the premises provided by MITA;
- Access to MITA's Service Call Centre for the reporting and resolution 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.

During this audit, the NAO noted that the Commerce Department has various other services and maintenance contracts with other third party suppliers. The NAO reviewed most of these services and maintenance contracts and recommends that the Commerce Department ensures that:

- These contain suitable Data Protection Clauses similar to the clauses issued by the OPM;
- All IT related contracts and agreements are still valid;
- All third party suppliers abide by the terms and conditions, in terms of response times and the provision of services.

The NAO noted that one of the services and maintenance contracts pertaining to a multi-function printer is endorsed with all the relevant details of the previous owner under the MITC. In this regard, the NAO recommends that the Commerce Department should ensure that all the services and maintenance contracts are kept up-to-date, and if necessary, a covering letter documenting any changes that is signed by both parties should be attached to the respective contract.

2.7 Network Infrastructure

A network infrastructure refers to the hardware and software resources of an entire network that enables network connectivity, communication, operations and the management of an enterprise network. A network infrastructure provides the communication path and services between users, processes, software application services and external networks.

The NAO was informed that the Commerce Department is connected to the MAGNET, via a fibre-optic link to MITA-01 Data Centre in St. Venera. As highlighted earlier, the network connectivity is monitored and maintained by MITA on a 24/7 basis as part of the core services contract, whereby the IT Unit is informed whenever there is a service disruption. Furthermore, MITA also maintains all the network hardware, including the Department's router and switches, and provides the necessary support on the Local Area Network (LAN) and WAN infrastructure.

In the meantime, the Commerce Department provided the NAO with a schematic diagram of the core switches together with site plans for each floor. The NAO noted that in total the Department has four network cabinets, whereby two network cabinets are installed at a distance from each other on each floor. The NAO is pleased to note that every cabinet is properly labelled and all the cabling is well organised. Furthermore, every network room is kept free from clutter and kept secure under lock and key.

Whilst reviewing the network setup, the NAO observed that the main networking cabinet is connected to a Universal Power Supply (UPS). This is regularly monitored by the Senior System Administrator who informs MITA for any hardware faults.

With reference to the LAN infrastructure, the NAO observed that the Workstation Contractor carries out the patching of network points (both from the workstation to the wall port and within the respective network cabinet) provided that the necessary information and documentation is available. The NAO is pleased to note that the LAN connectivity within the Commerce Department is restricted with port locking. Thus, when connecting a new workstation or moving an existing workstation from one point to another, the Workstation Contractor must raise a service request with MITA's Service Call Centre to ensure that the network connectivity is available. If the network connectivity is not available, then either the same request is escalated to the relevant Service Team or another service request is raised specifically for the issues encountered.

Finally, the NAO was informed that the Commerce Department has a third party ADSL Connection, which is only used every fortnight for Video conferencing. Thus, the Department must ensure that the Video conferencing equipment should only be connected to the ADSL connection if and when required. In the meantime, the NAO noted that the IT Unit has access to the ADSL login and password. In this regard, the NAO recommends that the ADSL password is periodically changed and the respective login and password are kept in a sealed envelope and stored safely.

Chapter 3

IT Applications

Chapter 3

IT Applications

This Chapter delves into some of the IT software applications being used by the Commerce Department. It includes both the IT software applications, which are solely being used by this Department together with other software applications, owned by different Ministries and commonly used within Government Departments. In this regard, and as mentioned earlier in Chapter one, the NAO has evaluated the seven major software applications listed below:

- Dakar;
- e-Bridge;
- Fleet Management System;
- License Management System;
- Stock Ledger;
- Trademark System;
- TMview.

3.1 Dakar

In 1996, the Government of Malta acquired its first inter-Ministerial Human Resources (HR) tool known as HRIMS. The latter, which was developed in-house by MITA, was introduced as a 'prototype' but continued to serve its purpose well for many years. However, the need for a replacement of this system was felt with the increasing demand for an improved and more powerful system.

Following the issue of Legal Notice 327/2009, the responsibility for the governance of the Government payroll was transferred from the Treasury Department within the Ministry for Finance to the Public Administration HR Office (PAHRO) within the OPM. During the same year, a tender was awarded by

MITA to Dakar Systems to replace the HRIMS application. The Dakar application contains basic HR functions and with the strategic shift towards one integrated HR/Payroll system, it brought significant change in data entry, as the two functions could be captured in one single database, and a drastic reduction of possible inputting errors.

Between January and March 2010, the Dakar Systems' personnel offered extensive training to employees within PAHRO on the various functions and aspects of the new Dakar payroll application. Furthermore, employees from two test sites (pilot Departments), together with various members from the Gozo Salaries Section, were also given training by Dakar Systems' personnel. In the meantime, a number of meetings were held to discuss the system's implementation plan, the data migration requirements from the old to the new application, the testing and parallel running processes, a DRP and business policies. Following these meetings, the Dakar application was installed on test servers housed at MITA and two PCs within PAHRO were linked to the Dakar application so that hands-on testing could be initiated.

During the last quarter of the year, the final preparations for the implementation of the Dakar payroll application were made and parallel running was performed during November and December 2010. The final testing of the system was completed during this period, and the User Acceptance Testing (UAT) report was finalised before the Dakar application went live in January 2011.

The Dakar application is a Client/Server system with both Windows and web interfaces. The Windows interface contains all the payroll system functionality, whilst the web interface contains a sub-set of the payroll system functionality. The latter is mostly used by the satellite Departments, whilst the former is used by the PAHRO and the Gozo Salaries Section to perform centralised and specialised functions, such as the maintenance of employees, system tables, payroll calculations, governance, user management and reports.

Furthermore, the Dakar application is hosted at MITA-01 Data Centre in St. Venera, which provides a secure access to the server. MITA monitors and maintains the server in terms of hardware, backups and storage of backup media. The backup media is stored in safe repositories at an offsite location.

During the course of this IT audit, the NAO noted that the system is accessible via a web browser over a secure connection (https) through a login and a password. The NAO was informed that the system can easily be accessed from home especially, if the end user has the teleworking facility. To date, the Dakar application is mainly being used by one officer within the Commerce Department but her superior can also gain access to the system, if and when required.

In the event that the end user forgets his/her password, a service request is raised with MITA's Service Call Centre to reset his/her password. The new password is sent by MITA to the PAHRO who in return forwards the new password to the end user. Upon first logon, the Dakar application prompts the end user to change his/her password, which must be set as complex with a minimum of eight characters in length as per the GMICT password policy[5]. Furthermore, the Dakar application will block access after a particular amount of unsuccessful tries and the password is set to expire over a period number of days.

[5] http://mita.gov.mt/en/GMICT/GMICT%20Policies/CIMU_P_0015_Password.pdf

Since the Dakar software application is managed by the PAHRO and is also being used by the Gozo Salaries Section and all the Government Departments, the system has different user access levels depending on whether the system is used by *"Thick Client"* users (PAHRO, Gozo Salaries Section or third party supplier) or *"Web Client"* users (PAHRO or Government Department authorised users).

Prior to the payroll calculation, the authorised users within the Government Departments can create, modify and delete payroll adjustment records. Once the payroll calculation is triggered by the PAHRO, no authorised user within the Government Departments can modify or delete any adjustment records. In this regard, the NAO was informed that the Dakar software application has audit trails in place on a large number of fields for the creation, modification and deletion of data. Thus, any changes to the system are being recorded. However, the NAO could not view any audit trails or how data is being recorded, since the authorised user within the Department does not have access to view these logs.

Ever since the Dakar application was launched in January 2011, a number of new functions, processes and procedures were continuously introduced into the system to increase efficiency and reduce any errors or bugs. In this regard, with the introduction of the new payroll, a new initiative was introduced, whereby employees in possession of a Government e-mail account would receive their payslips electronically. The new payslip was designed in A4 format to enable the inclusion of more details. Employees not in possession of a Government e-mail were asked to provide a private e-mail address for this purpose. On the other hand, employees who did not provide an e-mail account received the usual paper based 'abridged' payslip from their respective Department.

The Dakar application can generate a number of reports, which are only accessible by the PAHRO. However, during the course of this IT audit, the NAO was informed that a new reporting facility was provided to the Government Departments, whereby the authorised user can click on the *'payroll data history'* tab to view the payroll history for every individual working within the Commerce Department. In this regard, the authorised user can access an individual's payroll history, since the system was launched in 2011, and can re-issue/print an individual's payslip if and when required.

In the meantime, the NAO was informed that whenever a person retires or terminates his/her job, the Commerce Department will inform the Gozo Salaries Section by e-mail with all the relevant details. The same level of communication applies whenever a new employee joins the Department.

Apart from the Dakar payroll application, in the beginning of 2012 the Dakar AMS module was fully developed and tested. This module was added to the current Dakar application and was eventually launched by the end of 2012. The AMS module was designed to capture all absences data availed of by Public Service employees, such as vacation leave, sick leave, parental leave, study leave etc. It also includes a set of reports and a calendar showing all absences taken by a particular person, on a yearly or monthly basis in a graphical layout. In the meantime, a number of users within Ministries and Government Departments attended to training and after a brief period of parallel running, the AMS module went live in February/March 2014. In this regard, the NAO was informed that two officials within the Commerce Department attended to a two-hour training session on the use of the AMS module at the PAHRO and began inputting data of all the absences recorded in 2014.

Having said that, the NAO noted that the Commerce Department employees are still applying for any vacation leave through the use of manual vacation leave cards. Even though these requests are then inputted electronically into the AMS module, the Commerce Department have not divulged whether these vacation leave cards will be removed or maybe introduce a new procedure in the near future, for the application of leave within the Department.

At the time of this IT audit, the NAO was informed that all the vacation leave cards prior to 2014, of every individual within the Commerce Department, have to be inputted manually into the system. Unfortunately, due to the lack of resources, this process is being carried out after office hours but to date, the Commerce Department cannot quantify the effort required to input all the data. In this regard, the NAO recommends that the Commerce Department should establish a cut-off date, analyse the amount of vacation leave cards that needs to be processed and the effort required to input all the data, taking into consideration the resources available.

3.2 e-Bridge

The Malta Crafts Council was set up by virtue of Act XXI of 2000, with the aim to focus on the encouragement, promotion and regulation of crafts and craftspersons and entrepreneurs in dealing with Maltese craft products. Crafts forming part of Malta's historical heritage is given particular importance.

Through this Act, both craftspersons and entrepreneurs can actively participate to promote Maltese crafts. It is in the interest of every craftsperson and entrepreneur to register with the Malta Crafts Council to have the opportunity to be part of the efforts of this Council and to participate in the election of representatives on the Council, which takes place every two years. In this regard, any craftsperson or entrepreneur who is a citizen of Malta, or who is not a citizen of Malta but who has the necessary permits according to law to operate in Malta, may submit, on a voluntary basis, his/her registration with the Council. This can be done either by downloading the application form from the Malta Crafts Portal or by submitting the application electronically provided that the craftsperson or entrepreneur has his/her e-ID credentials. The number of craftspersons registered with the Malta Crafts Council as on 31st December 2013, stood at 1,010 whilst the number of entrepreneurs registered with the Council on the same date stood at 471.

To update and maintain the Malta Crafts Portal, the Commerce Department utilises the e-Bridge software application, which is an online Content Management System (CMS) that was developed by a local third party supplier. The aim of this e-Bridge application is to provide advanced tools for easy, quick and reliable administration of all website content and functionality. Thus, it offers the flexibility to manage all textual, graphical and multimedia content of the portal.

The Malta Crafts Portal provides the visitor with an opportunity to get to know about craftspersons based in Malta and Gozo and to view a selection of their works. At the same time, visitors are being informed about activities related to Maltese Crafts. The portal also offers craftspersons the opportunity to promote their products via the interactive directory.

The portal runs in a virtualised environment hosted at MITA's e-Government Framework. It is based on a scalable design and technical infrastructure to allow for future growth and the addition of new online services and features, such as the integration with the Department's internal systems. To provide a flexible and attractive interface, the portal front-end makes use of various technologies including ASP, .NET, Adobe Flash, Adobe Flex, XML, HTML, Cascading Style Sheets and JavaScript. On the other hand, the back-end of the portal was developed using .NET technologies. Furthermore, the e-Bridge application runs on an SQL Server hosted on a Microsoft Windows server environment.

During the course of this IT audit, the NAO interviewed and observed how the e-Bridge administrator of the Small Businesses and Crafts Directorate updates and maintains the Malta Crafts Portal. The e-Bridge software application, which is solely being used by the Commerce Department, is accessible through a login and password. However, the NAO noted that there is no password complexity, password history or password expiry rules in force, since the application is only used to update and maintain the Malta Crafts Portal. Whilst the administrator can add/modify user accounts or change passwords if a user forgets his/her password, the administrator can also delete a user account if a user no longer requires access to the system. In this regard, the NAO recommends that the e-Bridge software application should follow the GMICT password policy whereby user passwords should at least be complex with a mix of letters and numbers, should expire over a period number of days and a password history rule is applied so that passwords could not be re-used after expiry.

The e-Bridge software application has two different user levels, namely the *"normal"* user and *"super"* user level. In essence, a *"super"* user would automatically have full access rights, without the need to assign 'view', 'edit' and 'add' access rights on content and data manually. Nonetheless, these access rights can be individually set to every account, especially when there are a large number of e-Bridge users with segregated responsibilities and tasks, which would therefore warrant the administration overhead to maintain such access rights. However, this is not the norm at the Commerce Department, since one administrator with the assistance of three other *"normal"* user accounts are currently maintaining and updating the Malta Crafts Portal.

The NAO also noted that the e-Bridge software application provides an audit trail for all the data changes and can provide a log of any changes in the database. The log will consist of any tables and fields that were modified,, who made the change and when it occurred. A Data Mapper is used to track back all the changes happening to the object to be forwarded to the database. This method will return the list of changes for a particular object and maps these properties to a table in the database. The modified objects and the state of the old object will be both logged. All the audit logs are then forwarded to a separate database on the data server.

The e-Bridge software application provides structuring of content pages using templates, which are designed according to the requirements of the information to be displayed on the Malta Crafts Portal. It also supports a number of functionalities such as:

- Multimedia support for video and audio;
- Intrinsic integration with the Google site map submissions for additional search engine compatibility;

- Import/export from/to standard formats such as XML, spreadsheet and database files;

- Comprehensive website visitor reports, which are integrated with Google Analytics application.

The NAO is pleased to note that the Commerce Department has a good working relationship with the local third party supplier. The latter adheres to the SLAs stipulated in the maintenance contract and can access the portal remotely to provide the required maintenance and fix any urgent problems/ bugs that might crop up. In the meantime, the NAO also reviewed the *'Design and Development of the Malta Crafts Portal'* documentation. The NAO commends this documentation, as it went through the software development life cycle and provided a detailed explanation of each phase, including the application security controls in place, such as *'Cross Site Scripting Prevention'*, *'Injection Flaws (SQL Injections)'*, *'Malicious File Execution Attacks'* etc.

As highlighted earlier, the e-Bridge software application is hosted on a segregated virtualised environment at MITA-01 Data Centre in St. Venera. MITA monitors and maintains the hosting servers in terms of hardware, web services, backups and the storage of backup media.

3.3 Fleet Management System

In 2007, the FMMU within the Ministry for Finance was assigned the task of implementing the FMS in all Government Ministries and Departments. The system was initially developed by MITA as a standalone pilot project at the Ministry for Finance before it evolved into a server based system as the main source of management and control of all the vehicles utilised within the same Ministries and Departments. It also provides various other tools for management to enhance its control over vehicles.

As established in the Public Service Management Code, each Ministry or Government Department should have an officer/s in charge of the respective Ministry or Department's transport. In this regard, the Commerce Department has allocated a Senior Clerk to manage the data related to the Department within FMS and to communicate and liaise with the FMMU if the need arises, in order to ensure the smooth running of the FMS.

The FMS is running on a Microsoft SQL Server and is currently hosted on a secure virtualised environment at MITA-01 Data Centre in St. Venera. MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is regularly backed up. The NAO was informed that the system is backed up through the *"grandfather-father-son"* rotation scheme, whereby a full monthly backup to tape (*"grandfather"*) is scheduled on the first Friday of the month whilst a full weekly backup to tape (*"father"*) is scheduled on the remaining Fridays of the month. On the other hand, an incremental backup to disk is scheduled from Monday to Thursday. Thus, the *"grandfather"* set consists of 12 backup tapes, whilst the *"father"* set consists of four backup tapes. In total, 16 backup tapes are used and stored in an offsite location.

During the course of this IT audit, the NAO reviewed the FMS at the Commerce Department together with the Senior Clerk who uses this system. The FMS is accessed by a login and password. The latter must be changed upon first logon, whereby the password must follow the password complexity rule, which include a mix of letters and numbers. The NAO observed that the password expires over a

period of days, and the password history rule is enforced, whereby the last five passwords cannot be re-used. However, the NAO noted that the system does not block access to the system after a particular amount of unsuccessful tries. In the meantime, if the end user forgets his/her password or cannot logon to the system, a service request is raised with MITA's Service Call Centre. Through a specially designed password management module, which was recently developed by the third party supplier, when a new password is generated, MITA will send the new password to the end user via e-mail in clear text. The end user must then change the password upon first logon.

Whenever a user retires or no longer require access to the system, the IT Unit within the Commerce Department is informed and in turn will inform MITA accordingly. However, the NAO was informed that logins of employees on prolonged leave, career break or maternity leave are not removed or disabled, however access rights are disabled after 120 days. In this regard, the NAO noted that the FMS has three different user levels, namely:

- **Read-only access (Level 1)** – Users who have been granted read-only access can only view and thus no changes or inputting of data can be done by the end user;

- **Specific user access (Level 2)** – This user access level is defined according to the end user's specific task/duty within the particular Ministry or Department;

- **Administrator rights (Level 3)** – This user access level has full access rights to administer the FMS.

The NAO is pleased to note that the FMS has audit trails in place whereby a full track of all changes carried out are accompanied by a timestamp, old value, new value and the user who performed the change. However, since the FMS is not owned by the Commerce Department, the NAO was not in a position to review how the audit trails are being recorded.

Whilst reviewing the FMS, the NAO noted that the acquisition of vehicles must be carried out in accordance with the directives issued by the FMMU, as per instructions set out in the Public Service Management Code and in line with the Circulars related to the acquisition of vehicles, whether purchased, leased, hired etc. Once the Senior Clerk inputs the new vehicle into the system, the Ministry's DCS will have the sole responsibility to authorise that the vehicle can be furnished with fuel chits, maintenance etc. Without the DCS's approval on FMS, the status of the vehicle will remain inactive. In this respect, the DCS will exercise and have full control on the management of vehicles within the respective Ministry and its Departments. Apart from the issue of fuel chits, the FMS can store a history of the vehicle's related maintenance and any collisions or traffic fines incurred and when the Vehicle Roadworthy Test (VRT) and Road License is due.

The FMS also allows for the transferring of vehicles between Ministries, Departments or Sections. It also caters for the laying off vehicles and changing the status of vehicles to inactive or vice versa. No fuel transactions will be allowed once the status of the vehicle is set to inactive. The issuance of fuel chits is totally and fully dependent on the vehicle's odometer reading. If the odometer reading is not updated

into the system, a new fuel chit authorising the issuance of fuel will not be issued. In this regard, the NAO was informed that the fuel allowance for Directors and Director Generals is set to 150 litres whilst Permanent Secretaries have a limit of 175 litres a month. This does not differentiate between petrol and diesel engine vehicles. On the other hand, general use vehicles have no fuel thresholds in FMS, if the respective Ministries or Departments do not impose limits on their own vehicles. Having said that, the NAO noted that the FMS has in-built controls/limits on the issuance of fuel chits. Thus, every vehicle has a fuel quota per month and once these limits are reached, the system will block the issue of any fuel chits for that particular month. In the meantime, fuel prices are updated by the FMMU each time there is a change in the price of fuel.

During the course of this IT audit, the NAO reviewed the process involved in the issuance of fuel chits. In this regard, the NAO noted that when a new fuel requisition sheet is issued, it is printed twice on the same paper, in which the original requisition is given to the service station and the copy is retained by the Department. The original requisition is then sent back to the Department together with the invoice issued by the service station. Whilst going through this process, the NAO observed that the Commerce Department makes use of two service stations. However, one of the service stations is listed twice in the FMS under a different heading. Nothwithstanding the above, the NAO was informed that lately the Department was using only one of the listed names of the service station in question for the issuance of fuel chits. In this regard, the NAO recommends that the Commerce Department should liaise with the FMMU and rectify this problem by grouping all the data under one service station heading. Unless this is sorted out, having a service station listed twice under a different heading may lead to erroneous data in the issuing of reports such as to reconcile the number of fuel requisitions issued with the invoices received over a period of time.

In the meantime, the NAO was informed that the FMS is currently in the process of being migrated from a client server application to a web solution referred to as the *"Fleet Web Portal"*. The latter will be integrated with the current FMS, and although the functionality will remain the same, the web portal will include a number of enhancements. To date, even though the *"Fleet Web Portal"* was implemented at the Ministry for Finance and the Customs Department, the migration process from the current FMS to the new *"Fleet Web Portal"* is still in testing phase. However, some minor issues were raised and are currently being tackled by the respective third party supplier. Eventually, 99% of the current FMS users will start using the *"Fleet Web Portal"*, whilst the FMMU, MITA and the respective third party supplier will continue using the current FMS application.

Finally, the NAO was informed that the Ministry for Finance and the FMMU have an excellent working relationship with the third party supplier and the SLA timeframes stipulated in the service maintenance contract were always adhered to. Over the years, the FMS has been greatly improved and made much more user friendly with the implementation of a number of enhancements. In the meantime, to ensure the smooth running of the new *"Fleet Web Portal"*, the NAO is pleased to note that the third party supplier has already drafted a user's manual with all the relevant screen shots to help the existing and potential users familiarise with the new system.

3.4 License Management System

Following the enactment of the Trade Licences Act, 2001, police trading licences were devolved to different authorities. Therefore, the various authorities became the sole licensing authority for the activities they regulate, in line with the Government's policy to provide a *"One Stop Shop"* concept. In this regard, the Commerce Department is the competent authority to manage trade licences for:

- Self-employed who operate from non-fixed commercial premises;
- The operating of fixed premises for a commercial purpose, such as retailers, wholesalers and manufacturers;
- Market and street hawkers;
- Other commercial activities not otherwise regulated; and
- The organisation of commercial fairs and car boot sales.

The LMS is thus used by the Commerce Department to manage trade licences, in terms of their activity, payment history, reporting and to meet a variety of other business needs. Apart from the Commerce Department, the Local Councils have limited access to the LMS, whereby traders can renew their trading licence at their Local Councils offices, whilst the Law Courts and the Employment and Training Corporation (ETC) can only view data stored on LMS.

The LMS, which was developed by MITA, runs on a Microsoft SQL database and is currently hosted in a virtual segregated environment at MITA-01 Data Centre in St. Venera. MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is regularly backed up. The NAO was informed that the system is backed up through the *"grandfather-father-son"* rotation scheme, whereby a full monthly backup to tape (*"grandfather"*) is scheduled on the first Friday of the month whilst a full weekly backup to tape (*"father"*) is scheduled on the remaining Fridays of the month. On the other hand, an incremental backup to disk is scheduled from Monday to Thursday. Thus, the *"grandfather"* set consists of 12 backup tapes, whilst the *"father"* set consists of four backup tapes. In total, 16 backup tapes are used and stored in an offsite location.

During the course of this IT audit, the NAO reviewed the LMS at the Commerce Department together with a Senior Official responsible for the overall running of the LMS. The LMS application is accessible through a login and a password. Password complexity rules are enforced and all passwords expire after a specific period. Moreover, old passwords cannot be re-used after expiry, however, the system does not block access after a particular amount of unsuccessful logon attempts. In the event that a user forgets his/her password, one of the three LMS administrators within the Commerce Department will reset the end user's password. Upon first logon, the end user is prompted to change the new password provided.

In the meantime, whenever a user retires or no longer requires access to the system, one of the LMS administrators will disable the respective user access rights after 120 days and eventually delete these user accounts. Moreover, the NAO was informed that logins of employees on prolonged leave, career break or maternity leave are not removed or disabled, however access rights are disabled after 120 days. On the other hand, if a new user requires access to the LMS application, a service request is raised with MITA's Service Call Centre for the creation of a LMS user account. MITA will forward the respective login and password to the LMS administrator within the Commerce Department. The latter will then assign the access rights according to the user role. In this regard, the NAO noted that the LMS has three different user levels, namely:

- **Read-only access (Level 1)** – Users who have been granted read-only access can only view and thus no changes or inputting of data can be done by the end user;

- **Specific user access (Level 2)** – This user access level is defined according to the end user's specific task/duty within the particular Ministry or Department;

- **Administrator rights (Level 3)** – This user access level has full access rights to administer the LMS.

The NAO is pleased to note that the LMS has audit trails in place whereby a full track of all changes carried out are accompanied by a timestamp, old value, new value and the user who performed the change. In this regard, the LMS administrators can view these audit logs if and when required.

Whilst reviewing the LMS, the NAO observed how the Commerce Department manages trade licences, in terms of their activity, payment history, reporting and to meet a variety of other business needs. In this regard, the NAO was informed that a client, who intends to exercise a new commercial activity in order to secure a licence for a commercial activity under the Trading Licences Act (Cap. 441), must fill in the respective notification/application forms , which must be then handed-in to the Business Care Unit within the Commerce Department. The Business Care Unit will then input all the data submitted from the notification/application forms into the LMS. The Trade Licensing Unit, within the Commerce Department will then process the respective application forms and issue a trading licence within 10 working days. The latter is valid for one year and can be renewed online through the use of e-Forms, by cheque payable to the Trade Licensing Unit or at the Local Council offices. Prior to expiry, the trader is notified with a letter by post and has 60 working days to affect payment. In the meantime, the NAO observed that the issue of trade licences has increased drastically in 2013. As depicted in Table three, in 2013, 1,944 trade licences were issued when compared to 1,188 in 2012 and 1,198 in 2011.

[7] http://www.commerce.gov.mt/lics_forms.asp

Premises Based	Year		
	2011	2012	2013
New applications	416	398	1,097
Changes or Increase in Activities	68	100	42
Transfer of Licence/By Inheritance	381	330	101
Re-Activation of Licence	10	26	6
Non Premises Based	**Year**		
	2011	**2012**	**2013**
Registrations of Freelance Activities	113	179	414
Others	**Year**		
	2011	**2012**	**2013**
Street Hawkers	101	115	128
Market Hawkers	84	1	86
Marketing Agents	5	4	7
Buskers	20	35	63
Total	**1,198**	**1,188**	**1,944**

Table 3 - LMS Statistics

At the time of this IT audit, the NAO noted that since the business behind the trade licensing is continuously evolving, various processes and procedures were introduced throughout these years. In this respect, a number of enhancements, which were required in the LMS system were identified by the Commerce Department. These were supported with detailed documentation of a number of enhancements that were proposed by the Department, such as to improve the reporting functionality as per business requirements, to introduce new auditing mechanisms, and implement a new administrator module amongst others. The NAO commends these initiatives being triggered by the Commerce Department to continuously improve the system and adjust to new business requirements. The NAO is pleased to note that all these enhancements go through the software development life cycle before they are implemented through the change management process. Moreover, the local third party supplier also provides a detailed documentation on the deliverables, time scales and a description of what the change/enhancement will entail.

In this regard, the NAO is pleased to note that the Commerce Department has a very good working relationship with MITA and the local third party supplier who maintains the LMS applications. The local third party supplier adheres to the SLAs stipulated in the maintenance contract and can access the LMS application remotely to provide the required maintenance and fix any urgent problems/bugs that might crop up.

Finally, the LMS offers a sound reporting functionality. As long as the end users are provided with the necessary access rights, the LMS end users can issue various reports, such as:

- **Trade Licenses by Criteria (Street/Locality/Type)** – This report provides information about the license details, licensee contact details, business details sorted by the street, locality or type;

- **Renewals Generated Report** – This report provides a list of license renewal notices issued for a given year;

- **Withdrawn Licenses** – This report provides a list of withdrawn licenses for a particular year or all years;

- **Licenses Top Dues** – This report provides a list of pending licenses in descending order from the highest debtor to the trader who owes the least;

- **Payment reports** – This report provides a list of all the payments for a specified date range;

- **Applications/Notifications report** – This report can retrieve all the applications or notifications received for a specified period.

The NAO was informed that all the reports generated by the LMS can be exported to a spreadsheet by authorised users. In the meantime, the NAO commends the initiative taken by the local third party supplier and MITA to draft a *"User's Guide"* and provide a detailed documentation with all the relevant screenshots to the LMS end users, on how to generate the reports available through the LMS application.

3.5 Stock Ledger

The Stock Ledger software application was developed as an "interim application" required to meet the business and technical requirements stipulated in the *"Treasury Circular 06/2004 – Stock Control Procedures"*. The Stock Ledger software application was developed at a time when another Stock Control software application (Store_IT) was meant to be replaced, as it was based on old technology that could not meet Government requirements and adhere to the GMICT standards. In this regard, the Ministry for Finance together with the Treasury Department, intend to replace the Stock Ledger software application with a new Corporate Finance Management Solution, which is currently under adjudication process by the Director of Contracts at the time of this IT audit. It is estimated that the Stock Control, which is part of Phase one of the new Corporate Finance Management Solution, is estimated to be implemented by 2016.

The current Stock Ledger software application was developed by MITA upon request by the Ministry for Finance's Accrual Accounting Task Force and the Treasury Department. The NAO was informed that MITA is responsible for the overall maintenance and upkeep of the Stock Ledger software application, however, in light of the new system is currently under adjudication stage, no major enhancements are being carried out on this application.

During the course of this IT audit, the NAO interviewed and observed how the Stock Ledger software application was being accessed within the Commerce Department. The NAO noted that the Stock Ledger software application runs on Microsoft Access and is installed on the end users workstation. The system is accessible through a login and a password, however, there are no password complexity rules in place, passwords do not expire and the user account is not locked after a number of unsuccessful

logon attempts. Furthermore, there are no audit trails in place since the system is an 'interim' solution until the new Stock Control software application is implemented.

Furthermore, since the Stock Ledger software application is installed locally, the end user is responsible for his/her own PC or laptop and before logging off the Stock Ledger software application, the end user must take a daily backup and make sure that this backup is stored safely. In this regard, the NAO was informed that until recently, the Stock Ledger software application was being backed up locally on the PC or laptop's Hard disk. To ensure that the data is kept securely, the Department took the initiative to backup the Stock Ledger software application on the end user's home folder. The latter is hosted at MITA's segregated environment and is backed up daily. Whilst the NAO commends this initiative to safeguard the data, the NAO recommends that a copy of the backup is stored on an external device at least once a week in the event that the network is not accessible and the end user needs to input or retrieve data from the Stock Ledger software application.

Whilst reviewing the Stock Ledger software application, the end user explained that any receipts or issues of stock are recorded into the system. The NAO noticed that proper procedures are in place for receiving, checking and recording goods received. Thus, for every stock item, the end user must input the stock code, store location, Department name, type, category and unit of measure using a list from a dropdown menu and then save to create a *"Stock Ledger Card"*. On the other hand, the issues and receipts form is used to update stock movements for a particular *"Stock Ledger Card"*. The NAO noted that for every receipt and issue of the current stock, the balance of stock items is re-calculated automatically.

The NAO was informed that the officer in charge of the Stock Ledger software application, together with another official representing the accounts section within the Commerce Department, ensures that a stocktake is carried out at least once a year, usually at the end of the financial year. In this regard, all stock items have to be properly located and referenced with access restricted to authorised officials within the Department. The NAO recommends that any expensive stock items are located separately and in safer places. Furthermore, slow moving stock items and obsolete ones must be identified and located for appropriate valuation.

During the stocktake process, the officer in charge is to assess the current condition of the stock. The identification of stock condition is important, as each condition will carry its own valuation method. Thus, the following classification is normally used:

- Normal stock items;

- Unserviceable stock items that can be either spoiled, defective/damaged stock or obsolete/ expired stock;

- Surplus stock, that is, normal stock that the Department has no further use for and which cannot be used for any other alternative purposes. In this regard, the Department is to ensure that prior to such classification of stock it took all possible measures for its utilization including the re-selling to other Departments at a cost. However, the Heads of Departments must sanction this procedure.

Finally, the NAO noted that the Stock Ledger software application can generate three types of reports, namely the *"Stock Valuation report"*, the *"Summary Report by Stock Code"* and the *"Stock Ledger Report"*. All the reports can be then exported and saved in a spreadsheet. In the meantime, the NAO was informed that a *"Stock Valuation Report"* is issued every quarter and sent to the Treasury Department within the Ministry for Finance via e-mail on a generic mailbox. Prior to sending this e-mail, the end user prints this *"Stock Valuation Report"* and forwards it to his/her superior to ensure that it is correct. The report is then signed and filed accordingly within the Department.

3.6 Trademark System

A trademark is a word, phrase or symbol, or a combination of words, phrases, symbols or figurative elements that identifies and distinguishes the goods and services of one company from those of another. Organisations ranging from Small and Medium-sized Enterprises (SMEs) to huge multi-nationals use trademarks registration systems to protect their brands.

If an individual or a business requires trademark protection, this can be achieved by registering with the national, regional or international trademark offices. These trademark registration systems all provide legal protection, but are limited to the territories in which they operate. Thus, an organisation or individual that needs to do business in just one or two countries may choose to obtain protection by applying separately to the appropriate official trademark offices.

In the early 1990s, the Commerce Department commissioned MITA to develop an automated workflow system for trademarks to be used by the IPRD within the Department. The TMS thus provides for the basic processing of trademark applications, that is, from the inputting of data of each new application to the issue of the trademark's certificate of registration. The TMS application is currently hosted in a virtual segregated environment at MITA-01 Data Centre in St. Venera and has been supported by MITA throughout its 20-year life span. MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is regularly backed up. The NAO was informed that the system is backed up through the *"grandfather-father-son"* rotation scheme, whereby a full monthly backup to tape (*"grandfather"*) is scheduled on the first Friday of the month whilst a full weekly backup to tape (*"father"*) is scheduled on the remaining Fridays of the month. On the other hand, an incremental backup to disk is scheduled from Monday to Thursday. Thus, the *"grandfather"* set consists of 12 backup tapes, whilst the *"father"* set consists of four backup tapes. In total, 16 backup tapes are used and stored in an offsite location.

In Malta, the application for the registration of a trademark must be made with the Commerce Department, whereby the application is either received by post, e-mail or through the use of e-Forms. The application is then examined to ascertain that all the requirements for the registration of such an application are met. In this regard, if the applicant wishes to apply for a trademark in respect of different goods and services, the applicant must fill-in a different application for each category[7]. Goods and services are classified by the IPRD according to the International Classification of Goods and Services for the purposes of the registration of trademarks under the Nice Agreement[8]. The latter,

[7] https://secure2.gov.mt/ipo/Intellectual_Property_Office_Malta/Trademarks/tm_application_forms.aspx?ct=1
[8] http://www.wipo.int/classifications/nice/en/

divides the goods and services into 45 categories (or classes), namely classes 1-34 are associated with goods, whilst Classes 35-45 are associated with services.

Prior to submitting an application, the applicant, if in doubt, should check with the IPRD as to how his/her goods and services should be classified. The application for the registration of trademark must be then filled on the appropriate form and should contain the following:

- A request for the registration of a trademark;
- The name and address of the applicant;
- A statement of the goods and services in relation to which it is sought to register the trademark;
- A representation of the mark;
- The name and address of the representation or attorney, in cases where one has been appointed;
- A declaration claiming priority in cases where the applicant wishes to take advantage of an earlier application;
- An indication that the trademark is being used by the applicant or with his/her consent, in relation to those goods or services, or that the individual has a *bona fide* intention that it should be used;
- A statement containing the name or names of the colour or colours being claimed in cases where the applicant wishes to claim a colours as a distinctive feature of the mark; and
- A prescribed fee, which covers the cost of filing, registration and publication in the Government gazette.

Once the formalities are fulfilled, the application is then checked by the IPRD for compliance with requirements. A sign, which does not fall within the definition of trademarks, will not be registered as a trademark. In this regard, the registration of a trademark is refused if the trademark:

- Lacks distinctive character;
- It is identical with or similar to an earlier trademark, and although the goods or services are not similar to those in the earlier trademark, yet the registration would take unfair advantage of the distinctive character or repute of the earlier mark;
- Its use is prohibited in Malta by any enactment or rule of law;
- Is made up entirely of signs or indications which may serve, in trade, to designate the kind, quality, intended purpose, value, geographical origin, the time of production of goods or of rendering of services, or other characteristics of goods or services;

- Notwithstanding the above, the registration of a trademark is not to be refused, if it can be shown that before the date of application for registration, the trademark has acquired a distinctive character as a result of the use made of it in Malta.

During the course of this IT audit, the NAO noted that for every trademark application, a number is assigned manually into the TMS application since the system does not generate a trademark number automatically upon inputting the respective details pertaining to the trademark application. The corresponding trademark application number is then assigned to a physical file, which is used internally to insert all the necessary documentation pertaining to the trademark application.

When a trademark is registered, the Comptroller publishes the registration and issues a certificate of registration to the applicant. The duration of a registered trademark is 10 years, which commences from the date of registration. The trademark may be then renewed for further periods of 10 years at the request of the proprietor, after the payment of the renewal fee within not more than six months before the date of expiry. The renewal takes effect from the date of expiry of the previous registration. If the registration of a trademark is not renewed, then the Comptroller will remove the trademark from the register. At the time of this IT audit, the current registered trademarks found in the TMS application amount to 22,939.

In the meantime, the Commerce Department provided the NAO with a statistical report on the total number of applications received for the registration of trademarks and the total number of trademarks that were registered between July 2013 and July 2014. As depicted in Figure two, the total number of applications received for the registration of trademarks amounted to 880, of which 509 applications were received from residents, whilst 371 applications were received from non-residents. On the other hand, the total number of trademarks registered within that period amounted to 999, of which 475 were related to trademarks registered on behalf of residents, whilst 524 were related to trademarks that were registered on behalf of non-residents.

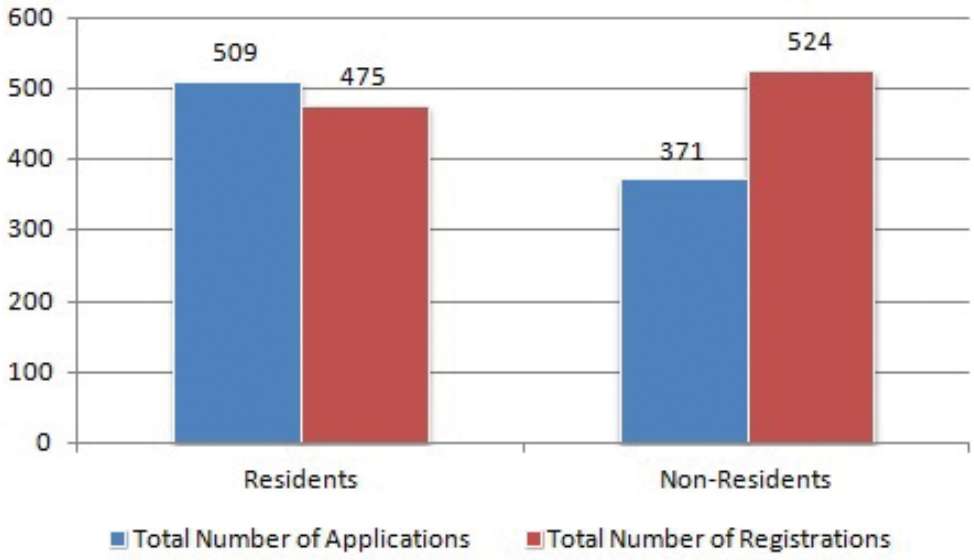


Figure 2 - TMS Report - July 2013 - July 2014

Whilst going through the TMS statistical report, the NAO queried on the high amount of trademarks registered on behalf of non-residents. In this regard, the Commerce Department explained that this amount does not reflect the amount of applications received within the stipulated period. Sometimes, the Commerce Department seek further information from non-residents before a trademark is registered locally. Thus, the total amount of 524 trademarks made in the name of non-residents is attributed to the applications received over a period of one year and prior to July 2013, which could not be registered until a trademark complies with all the requisites highlighted earlier.

In the meantime, while reviewing the TMS application, the NAO observed that the TMS is accessible through a login and a password, however the system will block access after a particular amount of unsuccessful logon attempts. All passwords expire after a specific period, but old passwords can be re-used after expiry in alternate between two previous passwords. In the event that a TMS user forgets his/her password, a service request is raised with MITA's Service Call Centre to reset the respective TMS password.

Furthermore, the NAO noted that TMS user accounts are not deleted or disabled whenever a user retires or no longer requires access to the system. Similarly, user accounts of employees on prolonged leave, career break or maternity leave are not removed or disabled. Moreover, the TMS application does not have any audit trails in place to record any changes made by the TMS users. In this regard, the NAO acknowledges the fact that the TMS application lacks audit trails, password security controls and that user accounts are not being managed accordingly. However, the NAO was informed that the TMS system will be replaced by a modern Back Office application, which will be provided by OHIM. The new system will be implemented in two stages and should be running live in the first quarter of 2015. Thus, the NAO recommends that the Commerce Department should ensure that the new application complies with the GMICT password policy, a full audit trail is in place and the new system complies with the software development life cycle process.

3.7 TMview

Companies work differently and have different needs. Many of them work locally, regionally and nationally. Others have international or global business needs. Logically they seek for different ways to protect their trademarks. Depending on the most appropriate type of protection, trademark protection and registration can be granted through the official trademark offices at National, International or European level. All these trademarks coexist and complement each other. Thus, businesses can consult all the trademark data by accessing individually the websites of the different official trademark offices. In doing so, businesses are confronted with a different layout, different languages and they may even be asked to pay for this consultation service.

In this regard, the OHIM took the initiative to create an internal portal to search the National trademark registers of all EU Member States and other participating trademark offices across the globe. This internal portal, known as TMview[9], is an online portal that allows any Internet user to search, free of charge, the trademarks of all participating official trademark offices. The TMview offers

[9] https://www.tmdn.org/

the functionality to download the information for the trademark that the Internet user is interested in and save the information in three different file formats, namely .pdf, .xls and .xml. Thus, the TMview can be used to:

- Carry out a trademark search;
- Check for the availability of your trademark name;
- Discover what your competitors are protecting; and
- Provide information to trademark examiners.

The TMview is multilingual and gives access to trademark applications and registrations of the participating official trademark offices. At the time of this audit report, the total number of trademarks found in the TMview amounted to 24,477,698. The latter is attributed to the number of trademarks provided by all the participating trademark offices, of which 52,062 are provided by the IPRD through the TMS application.

The accuracy of the data contained in the TMview is the sole responsibility of the participating official trademark offices or organisation providing it. In this regard, the integration of the Malta IP office with TMview necessitated the creation of the technological and organisational pre-requisites for data provision to this internal portal. In this regard, the NAO noted that the Commerce Department went through the software development life cycle before the TMview was launched, which included the Software Architecture Design and Analysis, Implementation Plan, Testing, and post review of the project. The IPRD within the Commerce Department, assisted by the services of the OHIM Deployed Manager, has provided OHIM with an initial upload of data and provides regular updates for all trademarks inputted into the TMS application. The latter was eventually launched within the Department in May 2013 and is currently being maintained by OHIM.

The TMview, which is hosted at MITA's segregated environment, reads from the current TMS application and writes into the TMview web services server, which is also hosted at MITA-01 Data Centre in St. Venera. The OHIM Deployed Developers have created an automated script to generate a file in .xml file format from the TMS application, which is then zipped and transferred on a shared directory. The TMview web services server will poll the shared directory and check whether the file has been generated. Upon detection, the TMview web services is updated with the new changes on to its own Microsoft SQL database hosted at MITA's segregated environment, with inserts for new data and any updates for alterations to existing data. As highlighted earlier, the file transfer has been automated and runs as a scheduled task on the TMview web services server. On days when no updates have taken place, an empty file will still be transferred. The NAO was informed this is usually the norm after office hours or over the weekend.

In the meantime, the NAO noted that the IT Unit, within the Commerce Department, monitors this file transfer on a daily basis by logging on the TMview application with administrator credentials and verify that no empty files were generated during office hours. In the event that an empty file is generated, the IT Unit will take a screen shot and send it to the OHIM Deployment Manager via e-mail. The

NAO asked whether this process can be automated whereby whenever the file is generated from the system, an e-mail is sent to the IT Unit. The latter will then view this e-mail and if the file generated is empty, the IT Unit will then log on to the TMview application, review the logs and inform the OHIM Deployment Manager accordingly. The NAO was informed that the IT Unit will be looking into this matter and discuss with the OHIM Deployment Manager whether this functionality is doable.

As highlighted earlier, the TMview application is currently hosted in a virtual segregated environment at MITA-01 Data Centre in St. Venera. MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is regularly backed up.

Chapter 4

Information Security

Chapter 4

Information Security

Information security refers to the processes and methodologies, which are designed and implemented to protect Information Systems and any confidential, private and sensitive information or data from unauthorised access, use, misuse, disclosure, destruction, modification or disruption. This may include amongst others a network disruption due to a Denial of Service (DoS) attempt. Information Systems that are infected by malicious software, such as malware, will allow a third party to gather sensitive information or gain unauthorised access to computer systems.

Thus, 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.

In this regard, the NAO analysed whether the Commerce Department adheres to Government security policies and procedures 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 effective security policy.

Although IT is responsible for providing the technology and mechanisms for protecting an organisation's data, a framework must be in place for making decisions as to what level of protection is necessary for any given data element (based on the criticality of the data). Without such a framework, there will be inconsistency in how data is protected, likely resulting in some data being under protected (thereby placing critical information assets at risk) or overprotected (leading to unnecessary costs). If the lifecycle of data is not defined, it will lead to data being retained longer than necessary (resulting in additional storage costs and possible legal liabilities) or being destroyed prematurely (leading to potential operational, legal or tax issues).

4.1.1 Information Classification

The classification of information is essential to any organisation, including the Commerce Department, and if everyone treats the same piece of information differently, this might have major negative consequences. Therefore, to provide the basis for protecting the confidentiality of data, an information classification policy must be closely tied to a security policy and an information disclosure policy. The information classification policy should:

- Describe the principles that need to be followed to protect information;
- Stipulate the manner through which one can distribute information; and
- List the people/entities to whom this information may be disclosed to.

In this regard, the NAO was informed that the Commerce Department does not have its own information classification policy. However, the Commerce Department refers to the GMICT information security policy[10], which explains how to protect the confidentiality of information by preventing the unauthorised disclosure of information (knowing that classified information can be accessed only by those authorised to do so). Thus, to protect the confidentiality of information, data can be classified under different security levels namely:

- **Top Secret** – Information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of Malta, the EU or one or more of its Member States;
- **Secret** – Information and material the unauthorised disclosure of which could seriously harm the essential interests of Malta, the EU or one or more of its Member States;
- **Confidential** – Information that is confidential by nature and could result in a significant impact on the Commerce Department or the Government if disclosed, modified or destroyed in an unauthorised manner;
- **Restricted** – Information and material that is restricted and the information asset owner may only disclose it to a particular named persons/roles on a need to know basis.

Depending on the level of classification, there are different rules controlling the level of clearance needed to view such information, how it must be stored, transmitted and destroyed.

4.1.2 Retention and Storage of Data

A data retention and storage policy defines how an Entity deals with maintaining its information. Such policy establishes a pre-determined set of time frames according to which an Entity retains the information collected. Furthermore, this policy includes the procedures for archiving the information,

[10] https://www.mita.gov.mt/en/GMICT/GMICT%20Policies/CIMU_P_0016_Information_Security.pdf

guidelines for destroying the information when the time limit has been exceeded and the special mechanisms for handling the information when under litigation, such as lawsuits or criminal investigations.

In this regard, the NAO was informed that even though the Commerce Department does not have its own data retention and storage policy, the Department refers to an HR retention policy that was issued by the Data Protection Unit, which all Government Departments need to abide with.

In the meantime, the Department adheres to the Data Protection Act 2001, Chapter 440 of the Laws of Malta, and the related legal notices, whereby the processing of personal data must be:

- Processed fairly and lawfully and in accordance with good practice;
- Collected for specific, explicitly stated and legitimate purposes;
- Processed strictly for the purpose it was collected;
- Adequate, sufficient and relevant in relation to the purpose of processing;
- Correct and up-to-date;
- Not kept longer than necessary.

4.1.3 Disposal of Information

Information Systems store data on a wide variety of storage media, including internal and external Hard disks, flash memory such as memory cards or USB pen drives, optical storage media such as CDs or DVDs and other types of removable media such as tapes or cartridges. Data can also be presented in printable format. To prevent unauthorised access, it is critical that data be rendered unreadable when documents or the drive on which data resides is no longer needed. Thus, any confidential electronic and paper information must be disposed of securely to minimise the risk of unwanted disclosure.

If confidential information is disclosed or lost this could cause harm or distress. This includes personal sensitive data as defined by the Data Protection Act, which is not in the public domain.

During the course of this IT audit, the NAO was informed that whenever a PC or laptop is no longer in use, any work related data is backed up on a CD/DVD and handed over to their respective Director or Assistant Director. The latter will check whether all work related data has been retrieved before the IT Unit can proceed in clearing all the data residing on the PC or laptop's Hard disk.

In this regard, the NAO commends the initiative taken by the Ministry's IMU in providing the Department's IT Unit with a data wiping software application. Whenever a PC or laptop will be disposed off or transferred to a different user within the Department, the IT Unit securely erases all the data residing on the Hard disk, using this data wiping software application, to ensure that no data can be

recovered from that drive. The third party service contractor is then called upon to re-image the PC or laptop with the Government standard software package.

In the meantime, the NAO recommends that the Department should ensure that the disposal of information on all types of media should follow the same route. Thus, a policy should be drafted and communicated internally describing the procedure to be adopted for the disposal of any confidential information, which may reside on paper, flash memory devices, CD/DVDs, through shredding, securing wiping and/or physical destruction etc.

4.2 Identity and Access Management

Identity and access management is the process of establishing and proving one's identity and to identify the applications one 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, the NAO observed how the Commerce Department adheres to these processes and what measures are 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.

In this regard, user accounts offer a way of managing access, providing user accountability and tracking the use of data, Information Systems and resources. Therefore, the management of user accounts and the monitoring of their use play an important part in the overall security of any organisation.

During the course of this IT audit, the NAO observed that all the requests for the creation, modification and deletion of user accounts to access any of the software applications or folders in use within the Commerce Department originate from the respective Directors or Assistant Directors. These requests are then forwarded to the IT Unit, who in return will then liaise with MITA, through the electronic Request for Service (eRFS) for the creation, modification or deletion of Government e-mail, Internet, Corporate system accounts in use within the Department, such as DAS, CdB, FMS, and Stock ledger. The same procedure applies when granting access to the end users on the applications solely being used by the Department, such as Trademarks and LMS and to shared folders residing on MITA's segregated environment. The user login and password is then sent to the IT Unit who will then forward it to the respective Director and Assistant Director. The latter will then forward the login credentials to the end user accordingly.

All user accounts are immediately suspended whenever a person retires, is discharged or transferred to a different Government Department. A list of officials who resigned/retired from the Commerce Department was provided to the NAO. During an on-site audit, the NAO verified that these user accounts no longer exist and noted that an e-mail account, which belonged to a user who had recently

retired still existed. In this respect, the IT Unit took immediate action and raised the necessary eRFS with MITA to delete the user account accordingly.

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 access or usage.

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

The NAO observed that most of the software applications selected during the course of this IT audit adhere to the GMICT password policy whereby a number of password security controls were taken into consideration. The password history settings were enforced in conjunction with the minimum age policy setting defined by MITA, to ensure that old passwords are not continually reused. However, this is not being applied on the e-Bridge and the Stock Ledger software application.

A minimum password length policy was defined so that end users cannot make use of blank passwords and the passwords should be set to a minimum of eight characters in length. All the passwords must meet the complexity requirements policy setting, which defines that new passwords meet basic strong password requirements, with a mix of letters, numbers and symbols. Similarly, the password complexity rule does not exist on the e-Bridge and the Stock Ledger software application.

Furthermore, almost every user account password expires over a specified number of days, with the exception of the e-Bridge and the Stock Ledger application user accounts. In the event that a user forgets his/her password, the end user must contact the MITA Service Call Centre to reset the password for Government Corporate systems such as e-mail, Internet, FMS, Dakar or DAS with the exception of the LMS, whereby the end user must contact the LMS administrator within the Department.

4.2.3 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.

The NAO observed that audit logs on most of the software applications selected in the audit report are enabled, whereby a secure audit record is created each time a user accesses, creates, updates, archives or deletes information from the software application. These audit logs uniquely identifies the user, function performed and the data and time the function was performed.

As highlighted in the previous Chapter, the Stock Ledger software application does not have any audit trails in place since the system is an ‘interim’ solution until the new Stock Control software application is implemented as part of the Corporate Finance Management Solution. Similarly, audit logs were not catered for when the TMS application was developed. However, the NAO was informed that the TMS system will soon be replaced by a modern Back Office application provided by OHIM.

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. It is normally disseminated through the normal communication channels either using e-mails, through the publication of leaflets and handbooks or communicated verbally, to ensure that information is conveyed to the appropriate users in a timely manner.

The NAO was informed that the Commerce Department does not provide security awareness to its employees, however they are regularly notified by MITA via e-mail on any security issues. Having said that, the NAO acknowledges that one of the best ways for any Department to improve information security is by raising awareness, training and educating everyone who interacts with its computer network, systems and information about the basics of information security.

The NAO recommends that such training initiatives can be offered as part of the induction session given to new employees and should also be part of an ongoing programme that seeks to ensure that all users are familiar with the information security policies and best practices that govern the use of IT assets. Awareness on security policies and best practices is normally communicated through the use of e-mails, publication of leaflets and handbooks or communicated verbally, to ensure that information is conveyed to the appropriate users in a timely manner.

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

Furthermore, the NAO suggests that IT Unit together with the Ministry's IMU should draft a set of computer security guidelines for all the officials within the Department. The aim of these guidelines should be to:

- Guide users as to how to protect their PCs or laptops and their personal information through the use of backups of important files, folder and offline mailboxes;

- Inform the users about the security risks of the Internet and highlight the appropriate actions that should be taken to reduce those risks;

- Explain how the network is set up whereby all the websites are being filtered and those deemed as unsuitable or undesirable are blocked;

- Provide some useful information on the proper use of e-mail, on how to avoid phishing, not to open any executable files and suspicious attachments and not to subscribe to unnecessary or unverified mailing lists;

- Provide hints on how to safeguard passwords and prohibit the sharing of logins and passwords.

4.4 Anti-virus Software

To effectively control and prevent the spread of malware, any Department should adopt a reliable Anti-virus software across its network infrastructure. The NAO observed that the PCs and laptops are installed with an Anti-virus software application as part of the Government standard software package.

In this regard, the Anti-virus software application is updated automatically by MITA. Even though MITA manages all the endpoints and provides all the necessary support, maintenance and updates, the NAO recommends that the IT Unit within the Commerce Department requests a periodic report from MITA to ensure that all the PCs and laptops within the Department are being updated with the latest definitions.

Furthermore, the NAO recommends that the IT Unit requests a quarterly report from MITA that would indicate which PCs or laptops were infected with malware and if the malware was removed. The report would help the IT Unit in identifying and taking the necessary actions required in the event that the same PC or laptop is continuously being infected by malware. In this regard, the IT Unit through the Ministry's IMU should educate the users and take the necessary measures to prevent similar instances, as these might pose a risk to the Commerce Department's network infrastructure.

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.

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

Operating system manufacturers usually provide regular product updates. These are classified as security 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 bypass a set of instructions that have malfunctioned. Unfortunately, a patch may add the potential for new problems. Most manufacturers would rather release a new program than patch an existing program.

The NAO observed that all the PCs and laptops within the Commerce Department are configured to automatically download and install product updates over the network. These product updates are being managed by MITA whereby hotfixes and patches released by Microsoft are distributed across the network. These are then downloaded and installed automatically on all the PCs and laptops within the Department. The NAO recommends that the IT Unit requests a quarterly report from MITA to verify whether all the PCs and laptops are being updated with the latest patches and hotfixes.

Chapter 5

IT Operations

Chapter 5

IT Operations

The continuity of operations and the 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, the NAO reviewed whether the Commerce Department 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 Security Controls

Today we live in a connected world and communication is a key requirement for all systems. The increased integration of systems requires a compulsive need to establish a fast and reliable communication that is as widespread as the Department and its business dealings. Since everything is connected to nearly everything else, Information Systems need to reach out to users, vendors and customers (irrespective of their location).

During the course of this IT audit, the NAO examined whether physical and environmental access controls are in place to safeguard all the IT equipment installed at the Commerce Department.

5.1.1 Physical Access Controls

Physical access control is a matter of who, where and when. Thus, having an access control determines who is allowed to enter or exit, whether an individual is allowed to exit or enter and when the individual is allowed to enter or exit. In this respect, physical access controls are designed to protect the computer hardware, software and network equipment from damage, theft and unauthorised access. Therefore, controlling physical access is just as critical as controlling logical access.

As highlighted earlier in Section 2.7, the NAO noted that in total the Commerce Department has four network cabinets, whereby two network cabinets are installed at a distance from each other on each floor. These network cabinets can be accessed by authorised personnel and are kept secure under lock

and key. Furthermore, the NAO observed that the room or the allocated space where the network cabinets are installed are well kept and free from clutter.

Intruder alarms and surveillance systems mitigate the risks of undetected physical intrusion by serving as a detective control as well as a deterrent for would-be intruders. The absence of these controls would increase the risk of theft and other criminal activities. At the time of this IT audit, the NAO was informed that the Commerce Department has two closed-circuit television (CCTV) cameras at the point of entry in two different levels. However, the footage is being stored at the National Statistics Office (NSO), which is situated next to the Department within the Lascaris Bastions, whilst the maintenance and running costs of these CCTV cameras are being shared between the Commerce Department and the NSO. Apart from the NSO and the Commerce Department, the NAO noted that the Lascaris War Rooms museum, under the responsibility of *Fondazzjoni Wirt Artna*, is also located within the Lascaris Bastions. In this regard, anyone who wishes to visit the Lascaris War Rooms or the NSO can pass through the Commerce Department's main reception. Even though there are signs to guide you through these buildings, any individual can easily roam about the Lascaris Bastions and pass through the Commerce Department's corridors. This poses a physical threat to the Department's offices as any individual with wrong intentions can easily enter any of the offices, even though the door offices are kept closed. In fact, it has been highlighted that at times theft of personal belongings, such as mobile phones, was reported. In this regard, the NAO recommends that the Commerce Department should immediately find ways on how to improve the physical access controls within the building.

The NAO was informed that discussions are currently underway with the Commerce Department and the Ministry's IMU, on how to enhance the physical access controls within the building. Furthermore, the NAO was informed that the Department intends to introduce CCTV cameras and install them at strategic points within the building. The Department is considering how to limit the access within the building to persons wishing to visit the Lascaris War Rooms or the NSO. Should the Department introduce CCTV cameras within the building, the NAO recommends that the new cameras are installed separately from the existing CCTV cameras and the recordings are kept securely within the Commerce Department. Furthermore, one has to keep in mind that the capturing and recording of images by means of a CCTV camera, leads to the identification of natural person and thus it constitutes the processing of personal data. By definition, this processing falls within the parameters of the local Data Protection Act. The NAO recommends that the data controller, within the Commerce Department, notifies the Data Protection Commissioner with the processing operation prior to physically installing the cameras and clearly define its purpose that shall be deemed proportionate with the rights to privacy of individuals.

Finally, since the Commerce Department is not equipped with any intruder alarms, the NAO was informed that after office hours, the Commerce Department makes use of the services of a watchman. The role of the watchman is to ensure that all the windows and main points of entries are locked and to carry out inspections on a regular basis.

5.1.2 Environmental Access Controls

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 IT audit, the

NAO examined the level of environmental access controls that exist within the Commerce Department and what measures are being taken to mitigate the above-mentioned risks.

The NAO observed that the Commerce Department is equipped with a number of fire extinguishers, which are placed at strategic positions within the building and are serviced and inspected annually by a local third party supplier. Even though a number of fire extinguishers are in place, the Department should ensure that officials are aware of how to handle the right type of fire extinguishers in the event of a short circuit or fire.

In the event of a power failure, the main networking cabinet that is connected to the MAGNET is equipped with a UPS. Furthermore, most of the PCs within the building are also connected to a UPS. The latter will safeguard the networking equipment and PCs connected to the UPSs from any power surges or unexpected shutdown. The IT Unit monitors these UPSs and immediate action is taken in the event that a UPS malfunctions.

Finally, the networking room where the main networking cabinet is installed is equipped with an air conditioning unit. The latter is kept switched on at all times and is monitored daily to ensure that the temperature is kept constant. In the meantime, the networking room is equipped with raised flooring that allows for easy access to telecom and data cabling for any maintenance services. Furthermore, raised flooring also prevents from flooding caused from external environmental factors or something as simple as a broken pipe from the main air conditioning unit for instance, thus reducing damage to the main networking cabinet even though the cabinet is installed at the far end of the room.

5.2 IT Service Management

The IT Service Management (ITSM) practices are important to provide assurance to the Commerce Department's officials and their respective superiors 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 supplier, 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.

As highlighted in the previous chapters, the IT Unit within the Commerce Department is the main point of contact between the Department and MITA or the local third party supplier that is providing a service. Thus, whenever a problem with a PC, laptop, printer, network connection or software application arises, the IT Unit is informed accordingly. In turn, the IT Unit will liaise with MITA's Service Call Centre and a service request is raised. A Call Reference Number is generated from MITA's Call Logging System and an e-mail is automatically sent by e-mail to the IT Unit's Senior System Administrator or the end user raising the request. The system administrator will then store all these e-mails on an offline

mailbox. Whenever a local third party supplier calls on site, a job sheet, which is handed in to the end user or the IT Unit, is stored in a file.

The NAO observed that the Department is satisfied with the overall level of support that is being provided by MITA or the local third party supplier. However, the IT Unit cannot quantify whether there are any recurring problems on the same hardware equipment or correlate incidents, which are similar in nature, to be able to justify hardware replacement or solve the root cause of the problem. Thus, the NAO recommends that at least the IT Unit keeps track of all the hardware related calls raised in a simple centralised spreadsheet. In this regard, the IT Unit could easily trace when a problem was first encountered, whether repetitive calls were made and when the problem was solved.

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 be developed to address the error state and prevent future occurrences of the related incidents.

Incident management and problem management are related but they have different objectives. Whilst problem management's objective is to reduce the number or severity of incidents, incident management's objective is to return the effected business process back to its "normal state" as quickly as possible. In this respect, MITA's Service Call Centre through their Call Logging System handles both incident and problem management.

As depicted earlier in Chapter three, the local third party suppliers adhere to a change management 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.

Most of the software applications that were selected in this IT audit report are hosted at MITA-01 Data Centre in St. Venera. MITA notifies all the parties concerned with the plan for the implementation of any changes that may affect the server or the virtual environment where the software application is hosted. These changes can even be delayed by MITA to allow a third party supplier to take remedial action as may be necessary in order to ensure that the proposed changes have no impact on the system. However, the NAO observed that MITA's services contract stipulates that it reserves the right to proceed with the implementation of the changes, in particular where the changes are deemed by MITA to be of a critical nature.

5.3 E-mail and Internet Services

The NAO considers e-mail and Internet services 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, resulting in increased productivity, a reduction in costs and better delivery of services.

Furthermore, e-mail has become an important component in an OA system. In this regard, e-mail facilitates the exchange of information, speeds up the decision-making process and reduces paperwork, resulting in increased productivity, a reduction in costs and better delivery of services.

The Commerce Department's e-mail and Internet services are being provided by MITA through the Government's communications backbone, MAGNET. In this regard, the NAO noted that the Commerce Department adheres to the *"Electronic Mail and Internet Services Directive"* that was issued by the former Central Information Management Unit (CIMU) in 2003.

The NAO observed that almost every official within the Commerce Department was provided with an e-mail and Internet account. The directive highlighted earlier stipulates that the e-mail service is provided for official business use only and is deemed the property of the Department. Thus, any e-mail, including attachments, that is created, sent, received or printed via the e-mail service, becomes the property of the Department. Furthermore, the personal use of e-mail is allowed only in exceptional cases and provided that this does not interfere with the performance of the account holder's duties or those of other account holders. In the meantime, the NAO was informed that to-date the Commerce Department has 11 generic e-mail accounts which are accessed by specific end users within the Department. All the end users who have been granted access to these generic e-mail accounts are responsible for the upkeep of these accounts in terms of e-mail correspondence, mailbox size and storage of offline mail.

Similarly, every user is responsible and held accountable for Internet activities carried out. 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 should not disclose the password or use someone else's password.

In this regard, 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 counterfeit. To this effect, any attempt to send or cause such counterfeit e-mail to be sent to or through the MAGNET is unauthorised.

The NAO recommends that the IT Unit should periodically remind all the officials who own an e-mail or Internet account within the Commerce Department, about the salient points highlighted in the *"Electronic Mail and Internet Services Directive"* especially the restriction on the use of e-mail and Internet services as depicted in Appendix D.

Furthermore, during the course of this IT audit, the NAO observed that offline mailboxes of personal or generic e-mail accounts are being stored locally on the end user's PC or laptop. In this regard, the NAO recommends that the Ministry's IMU together with the Department's IT Unit should provide guidelines to all the officials within the Department, on how to backup and securely store offline mailboxes.

5.4 e-Forms

An e-Form is a computer program version of a paper form. Aside from eliminating the cost of printing, storing and distributing pre-printed forms, and the wastage of obsolete forms, e-Forms can be filled out faster because the programming associated with them can automatically format, calculate, look up and validate information for the user.

As part of the e-Government vision, in 2012 the Government of Malta enhanced its technical infrastructure with the launch of an e-Form platform to serve as a single point of contact for the provision of online Government services. A uniform *"look and feel"* interface was created to give the impression of a single reference point for the public to access the Government services online. Most of the e-Forms exist in parallel with the traditional paper based forms and thus they are kept in synch until the paper-based forms are deemed obsolete and can be retired. In this respect, the use of e-Forms offer a number of advantages, namely:

- **Convenient** – e-Forms are available at your convenience. They can be filled-in and submitted from the comfort of your home 24/7 thus avoid waiting in line at Government offices;

- **Practical** – Certain information submitted will be asked only once. Thus, there is no need to refill whole sections since the information will be saved and can be re-used across a number of e-Forms;

- **Easy to use** – e-Forms are highly accessible and easy to use. They comply with international form standards and provide a familiar 'look and feel' as other Government services;

- **Informative** – There is no need to phone a Government Department to check on the status of the form. The e-Form keeps you informed about progress during processing.

During the course of this IT audit, the NAO was informed that the Commerce Department has 10 e-Forms that can be used for the application of a trading licence and other services as highlighted below:

1. **Busker licence application form (Form O)** – Selling by busking is permitted when a person acting as a busker within any street produces on site and sell work of art on site, must submit an appropriate form with the Trade Licensing Unit. No objects are placed on the pavement and the use and provision of public utilities is prohibited. Moreover, no selling by buskers that sell artefacts or rendering of this service must be carried out in Valletta, especially in Castile Square, in St. George's Square, in St. John's Square and in the Bus Terminus including St. James Ditch;

2. **Application to register a commercial activity under the Trading Licences Act (Cap 441 of 2002) and subsidiary legislation (Form A1)** – Any person who will be carrying on a commercial activity other than from commercial premises, which activity is not regulated under any other act, shall be registered in accordance with the provisions of any regulations as may be prescribed. Examples include freelancers who perform their commercial activity from home or who alternatively visit

the client's at the client's own property to carry out the proposed activity for which they would submit the registration;

3. **Application for a licence to exercise a new commercial activity under the Trading Licences Regulations (Form C)**;

4. **Late night shopping permit notification (Form K)** – Notwithstanding the established business hours, any commercial activity can be extended up to 22:00 on any other day of the week being either Thursday, Friday or Saturday. Provided that late night shopping in any such day shall only be allowed after the licensee had applied in writing;

5. **Notification or Application for a licence to exercise a new commercial activity in order to secure a licence said commercial activity under the Trading Licences Act (Cap. 441)**;

6. **Application for a market hawker under the Trade Licences Act (Cap. 441 of 2002) and subsidiary legislation (Form I)**;

7. **Marketing Agent – Licensing of commercial vehicles used for the sale of goods as part of licensed commercial activity (Form L)** – The licensee of an already licensed commercial activity may request the permit for the use of the commercial vehicle for the sale of goods by retail, by employees or an agent on behalf of the licensee. Such licence shall be required for each and every vehicle used for the exercising of such retail. This license shall not entitle any person to act as a market hawker;

8. **Obtaining an auctioneering licence under the Auctioneers Act Application** – This application is used by a person to request to be licensed to conduct public sales by auction but does not include an auctioneer of animals, including fish, whether dead or alive, food or agricultural produce;

9. **Register a collecting society application** – To establish and operate societies for the collective administration of copyright;

10. **Application for a street hawker under the Trade Licenses Act (Cap. 441 of 2002) and subsidiary legislation (Form H)** – A license is required in order for any person to lawfully carry out a commercial activity from any street. The license refers to a street as any road, alley, square, fortification or other place of public passage.

In the meantime, the NAO enquired about the extent usage of the above e-Forms. From the statistics obtained between July 2013 and July 2014, the NAO observed that these e-Forms are hardly being used. As indicated in the table below, only four e-Forms are being used out of the 10 e-Forms found online.

Reference	e-Form Name	Status	e-Forms Submitted
SDA020	Busker licence application form (Form O)	Live	0
SDA031	Application to register a commercial activity under the Trading Licences Act (Cap 441 of 2002) and subsidiary legislation (Form A1)	Obsolete	0
SDA032	Application for a licence to exercise a new commercial activity under the Trading Licences Regulations (Form C)	Obsolete	0
SDA034	Late night shopping permit notification (Form K)	Live	4
SDA036	Notification or Application for a licence to exercise a new commercial activity in order to secure a licence said commercial activity under the Trading Licences Act (Cap. 441)	Live	1
SDA037	Application for a market hawker under the Trade Licences Act (Cap. 441 of 2002) and subsidiary legislation (Form I)	Live	0
SDA038	Marketing Agent – Licensing of commercial vehicles used for the sale of goods as part of licensed commercial activity (Form L)	Live	2
SDA040	Obtaining an auctioneering licence under the Auctioneers Act Application	Live	20
SDA050	Register a collecting society application	Live	0
SDA710	Application for a street hawker under the Trade Licenses Act (Cap. 441 of 2002) and subsidiary legislation (Form H)	Live	0

Table 4 - e-Forms Submissions

As can be seen from the above table, there are two forms (SDA031 and SDA032) which are obsolete and were both replaced by SDA040. Even though these two forms were no longer in use, they are still listed in the Government e-Form portal as the form might still being processed by the respective Ministry, Department or Entity. Having said that, as highlighted earlier in Section 2.3, in the 2014, the Commerce Department has allocated the sum of €50,600 as expenses that will be incurred for the running of these e-Forms.

In this regard, the NAO suggests that the Commerce Department should try to identify possible reasons for the low usage of e-Forms by the audience required. The NAO feels that part of the reason may be the lack of marketing of such e-Forms given the fact that the application forms can be downloaded from the Commerce Department website but are not directed to the e-Form platform. The NAO also

believes that another reason for the low usage of these e-Forms may be due to the proliferation of the e-ID amongst the targeted audience. The NAO however, noted that the new ID cards are currently being rolled out, whereby every ID card holder will be provided with e-ID credentials. Furthermore, the NAO recommends that the Commerce Department reviews the current e-Forms and ensures that they are all updated and accompanied with a proper workflow, especially in view of a possible increase in e-Forms usage as a result of a wider distribution of e-ID in the coming months.

5.5 Web Filtering

A web filter is a program that can screen a website and determine whether some or all of it should be displayed or not to the user. The filter checks the origin or content of a website against a set of rules provided by the supplier or person who has installed the web filter. A web filter allows an organisation or individual user to block out pages from websites that are likely to include objectionable advertising, pornographic content, spyware, viruses and other offensive content.

MITA, being the Government Internet service provider, have adopted the *"Web Filtering Directive"* that was issued by the former CIMU in 2003. The aim of this directive is to setup methods for controlled access to Internet websites based on Government needs. The directive addresses the legal risk to Government and the productivity of Government Internet account holders.

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

5.6 External Communications

External communication can be defined as the exchange of information and messages between an organisation and any other Organisation, Department or Entity. Whilst traditional print methods of communications are still common, modern technology has changed the face of external communications, and the Internet has become a valued resource in reaching the public. Websites are created to offer informative information on the organisation and the products and services being offered. Social media such as Facebook and blogs are an easy way to reach target demographics and are a cost-effective means of promotion. However, with interactive technology there is also the possibility of public backlash, such as negative comment posting. In the long run, the benefits far outweigh the risks, as technology is far-reaching and allows the Department or Entity to communicate with audiences all over the world.

During the course of this IT audit, the NAO looked into how the Commerce Department is managing its communication tools, namely the official Department's webpage, the Malta Crafts Portal and two Facebook pages.

5.6.1 The Commerce Department Website

The Commerce Department website is accessible through the following Uniform Resource Locator (URL) **http://www.commerce.gov.mt**, which is hosted and backed up by MITA and complies with the Government's *"Website Content and Presentation Standard"* GMICT S 0051-1:2012[11].

During the course of this IT audit, the NAO reviewed how the Department is maintaining its website in providing a detailed description of the different units that fall under the Department's organisational structure. It thus provides valuable information to the public on the services offered by the Department, such as the issue and registration of trademarks and designs, issue of trade licences, importation of goods, exportation of dual-use items and military equipment and other services. The website also offers links to the National IP Portal and to the Malta Crafts Portal.

Whilst reviewing the Commerce Department website, the NAO noted that:

- The Trade Services Directorate tab has broken links to the SIGL website and to the Malta Maritime Authority website;
- The Trading Licenses forms can be downloaded from this website. However, there are no links to the e-Government portal, whereby an individual can submit an application online;
- There is no reference to the Commerce Department's Facebook pages.

In the meantime, the NAO was informed that the IT Unit together with the Ministry's IMU are developing a new website to replace the current website by the end of February 2015.

5.6.2 The Malta Crafts Portal

The Malta Crafts Portal is accessible through the following URL **https://secure3.gov.mt/maltacrafts/,** which is hosted and backed up at MITA, whilst the back-end is being provided by a local third party supplier. As highlighted earlier in Section 3.2, the Malta Crafts Portal is being managed by the Small Business and Crafts Directorate within the Commerce Department, through the use of the e-Bridge software application.

This portal provides information about craftspersons based in Malta and Gozo and to view a selection of their works. At the same time, visitors accessing this site are informed about activities related to Maltese Crafts. It also offers craftspersons the opportunity to promote their works via the interactive directory.

Whilst reviewing this portal, the NAO noted that this portal also complies with the Government's *"Website Content and Presentation Standard"* GMICT S 0051-1:2012. Overall, this portal is very attractive and one can easily find a craft or craftsperson through the use of drop-down menus by

[11] https://mita.gov.mt/en/GMICT/GMICT%20Policies/GMICT_S_0051-1_Website_Content_and_Presentation_Standard_v5.0.pdf

selecting a craftsperson, craft category, craft sub-category, by locality or by typing a particular keyword. Furthermore, an individual can even register online as a craftsperson through their e-ID credentials or by downloading an application form and submitting it to the Malta Crafts Council. In this regard, the NAO commends the Small Business and Crafts Directorate efforts in maintaining its database and uploading it through this portal.

In the meantime, the NAO noted that under the Publications tab, one could download official newsletters that were published by the Malta Crafts Council dated back to 2004. Furthermore, one can only view the front covers of the two editions of the *"Directory for Craftsperson and Entrepreneurs"* that were published in 2003 and 2007, since the hard copies of these directories can only be collected from the Commerce Department. Similarly, under the library tab, the NAO noted that one could download and view a list of crafts publications as at 30th October 2012. In this regard, the NAO recommends that the Commerce Department ensures that these tabs are updated if new directories or newsletters were recently published.

5.6.3 Facebook Pages

Nowadays, various entities worldwide regularly rely on social media to engage with their customers. Thus, social media can be defined as the social interaction among people in which they create, share or exchange information, ideas and pictures/videos in virtual communities and networks.

In this respect, the NAO acknowledges the fact that social media, such as Facebook, may help Government Departments or entities in achieving their mission and if leveraged to its fullest, may create the opportunity for greater collaboration between Entities and Departments. Furthermore, it helps management in decision-making, engender more experimentation and offer a tool through which a Government Department or Entity gets timely response from the public. At the time of this IT audit, the Department manages two Facebook pages, namely the Malta Crafts and the National Enterprise Support Awards (NESA) pages.

The NESA Facebook page was launched in 2009 and has 87 likes, mostly from the 25-34 years old age group. The Small Business and Crafts Directorate within the Commerce Department is currently managing this page, which was created by the Enterprise Policy Directorate within the MEIB, with the aim to promote the NESA. The latter rewards those entities, which support entrepreneurship and the promotion of enterprise growth. The competition, which is held annually, puts the spotlight on the role of the public sector at the local and national level in creating the right environment for business and boosting their development with specially conceived projects.

On the other hand, the Malta Crafts Facebook page was recently launched in October 2014 and replaced the Malta Crafts Council Facebook page, which was launched around two years ago. At the time of this IT audit report, the Malta Crafts Facebook page has zero likes and only serves as a link to the Malta Crafts Portal.

The Commerce Department should be aware of the potential of social media as a modern communication channel. In this regard, the NAO recommends that the Department promotes these

two Facebook pages by providing links from their respective websites and ensure that these pages are kept updated.

5.7 Risk Management

At the time of this IT audit, the NAO observed that the Commerce Department does not have a formalised Business Continuity and Disaster Recovery plans at the Department level. On the other hand, a BCP and a DRP cover most of the software applications selected in this report, as per MITA's SLA. In this regard, the NAO noted that MITA has implemented a number of measures to mitigate the risks involved in the event of a disruption or total failure in the Department's IT systems and network connectivity. Furthermore, all the software applications hosted at MITA are being backed up daily and all the backup media are being stored in an offsite location.

The NAO has however noted that in the event of a total system failure, the Commerce Department will adopt a manual process whereby the end user will take note of any activity that was carried out and when the systems are restored, all the data is then inputted in the respective software application.

Thus, the NAO suggests that the Commerce Department should perform a Business Impact Assessment and a Risk Assessment exercise from which a BCP and a DRP can be drafted at a Department level as highlighted in Appendix D.

5.7.1 Business Impact Assessment

A Business Impact Assessment is a critical step in developing a BCP. The Business Impact Assessment is an analytic process that aims to reveal business and operational impacts stemming from incidents or events. A Business Impact Assessment should lead to a report detailing likely incidents and their related business impact in terms of time, resources and money. This report should give an understanding of the impact of non-availability of the IT systems and components and how will this affect the 'modus operandi' within the Commerce Department.

The Business Impact Assessment process is based upon the information that is collected from the key persons of every Directorate within the Commerce Department. The information can be collected using different approaches. One of the popular approaches is the questionnaire approach whereby a detailed questionnaire is circulated to key users. Another alternative is to interview groups of key users. The information gathered during these interviews or from the questionnaire response is tabulated and analysed for developing a detailed Business Impact Assessment plan and strategy.

Furthermore, the NAO recommends that the Commerce Department lists and reviews its critical and non-critical functions. For each function, the Department 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 a disaster.

After going through this process, the Commerce Department should then determine a recovery strategy. This will identify the best way to recover each system or critical function in case of an interruption, including disasters, and provide guidance based on which a detailed recovery procedure is to be adopted.

5.7.2 Risk Assessment

The NAO believes that a cost-effective BCP and DRP need to be part of a disciplined risk management approach, which should include an analysis of business processes, and the risks that these processes face. A Department or Entity that fails to identify their risks or processes, can neither manage the risks nor realistically plan for their consequences.

The NAO recommends that the Commerce Department should carry out a risk assessment to analyse the value of their assets, identify threat to those assets and assess the level of vulnerability to those threat. Fires, floods, acts of terrorism/sabotage, hardware/software failures, virus attacks, DoS attacks, cyber crimes and internal exploits are all examples of the types of threats that are to be analysed assigning a probability assessment value to each.

Thus, the NAO suggests that a risk analysis is carried out to define preventive measures that will reduce the possibility of these threats occurring and to identify countermeasures to successfully deal with those threats if and when they develop. Therefore, a well-defined, risk-based classification systems needs to be in place to determine whether a specific disruptive event requires initiating a BCP or a DRP.

5.7.3 BCP and DRP

The primary objective of a BCP is to protect the Commerce Department in the event that all parts of its operations and/or Information Systems are rendered unusable and to help the Department recover from the effects 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 required to assure high availability and system reliability based on the inputs received from the Business Impact Assessment and Risk Assessment exercise.

Whilst a BCP refers to the activities required to keep the Commerce Department's operations 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 final result is to identify any improvements required in the Disaster Recovery strategy, infrastructure and the recovery processes established in the DRP.

Chapter 6

Management Comments

Chapter 6

Management Comments

The following comments were submitted by the Commerce Department by way of Management Comments.

General Comments

It would have been ideal if the views/considerations of MEIB CIO were also taken into consideration during the course of the IT audit in particular noticing that both the CIO and IMU are often referred within the final report. The CIO is responsible of all ICT within the Ministry including Commerce Department IT and therefore has a more holistic insight on the IT operations and IT-enabled investments to ensure that IT is successfully delivering the business requirements.

Specific Comments

IT Strategy Plan

IT plans are depicted on a yearly basis based on the budget allocation for the year. Presently MEIB CIO is in the process of drafting a three-year Ministry ICT strategy plan in which the Commerce Department IT strategy will be encapsulated.

Printers

A study by the IMU was carried out to establish the current state of play and to determine the requirements in order to reduce the amount of local printers. This project will be implemented in 2015 pending availability of funds.

Hardware and Software Inventory

One needs to point out that the hardware and software inventory is kept within a database system, which is mainly maintained by the IMU. The Commerce Department IT Unit has access to such system.

Furthermore, the IMU already carries out periodic audits to assess software applications and software licenses within the whole Ministry including the Commerce Department.

Trademark System

The new IP system was launched in mid-December 2014.

Security policy

This policy is being drafted by MITA together with a number of new security policies, which eventually will be adopted by the Ministry and Commerce Department. Such policies will officially be adopted government wide by mid next year.

Security Awareness

Occasionally Information Security awareness mail shots and posters are forwarded to all Government users. It is highly recommended that all users within the Ministry attend the Information Security awareness training provided by the CDRT.

e-Forms

All Commerce Department e-Forms were developed following a business analysis review and workflows were re-engineered in line with business requirements. Although the uptake of the e-Forms within the Commerce Department is not most favourable, the e-Forms offer an alternative and efficient service to citizens, which unquestionably are in line with Malta's e-Government strategy.

Offline mailboxes and generic email

One needs to point out that instructions/guidelines on how to backup and securely store offline mailboxes are periodically communicated to all users within the Ministry including the Commerce Department. Furthermore, an exercise is being carried out to identify those users who keep critical business information on their respective hardware in order to provide an online storage facility in which amongst other data offline mailboxes can be stored as from Q2 2015.

BCP & DRP

Both the drafting of the BCP and the drafting of the DRP will be identifiable tasks within the Ministry ICT strategic plan as explained above.

BIA & RA

The Business Impact Analysis and Risk Assessment exercise will also form part of the Ministry ICT strategic plan.

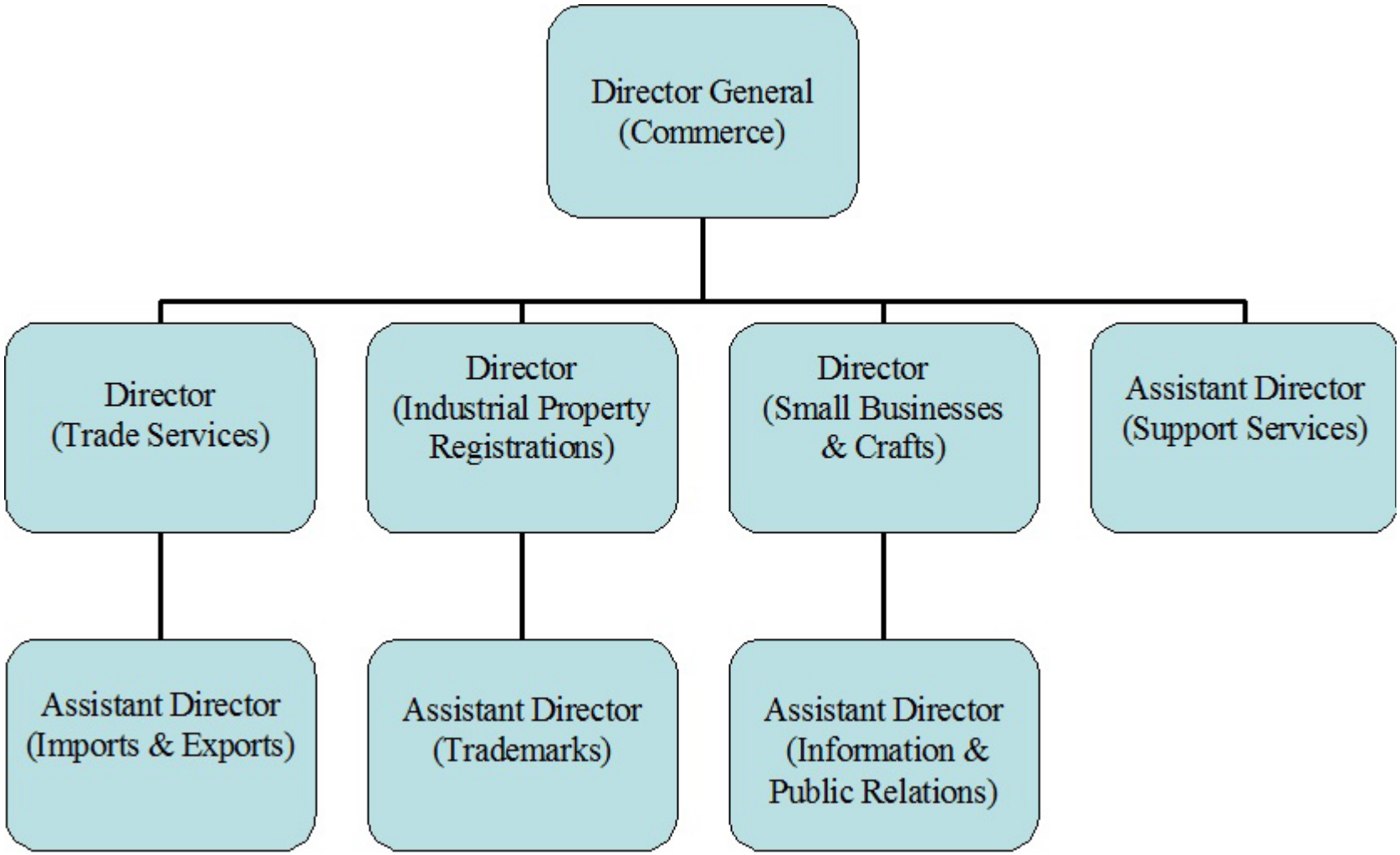
Maintenance

The IMU on a quarterly basis extracts related information from various tools provided by MITA such as the CIO portal and Marvel system to identify/analyze trends and calls of a particular nature, which collectively may indicate a common source in order to take all necessary action accordingly.

Appendices

Appendix A

Organisation Chart



Appendix B

COBIT Controls

COBIT 4.1 defines IT activities in a generic process model within four domains[12]. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate as depicted in Figure three. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

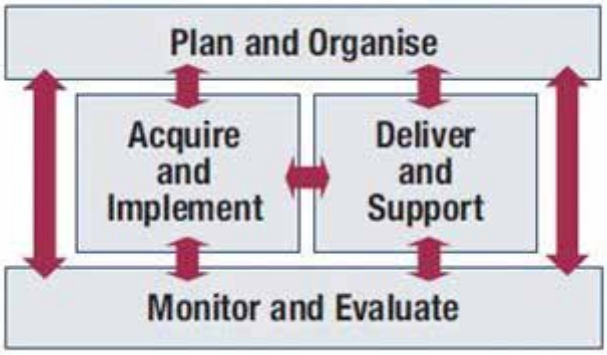


Figure 3 - COBIT Controls

Plan and Organise Domain

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.

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

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

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

Acquire and Implement Domain

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.

Deliver and Support Domain

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 Domain

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.

Appendix C

Restrictions on use of e-mail and Internet Services

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;
- Use another user'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, including 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;
- 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.

Restrictions on use of Internet services

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

- Create, willingly download, view, store, copy or transmit pornography and any other activities that are illegal, discreditable, offensive, and discriminatory or prohibited by law;
- Conduct or participate in crimes of any sort, example computer hacking, theft of proprietary data etc;
- In particular, authorised users are to refrain from seeking to impair any Internet content filtering facilities.

Appendix D

Business Continuity and Disaster Recovery Plans

A BCP should:

- Be consistent with the Commerce Department'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 the Commerce Department, 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 the Commerce Department'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;
- Identify the methods of communication among the key stakeholders;
- Implement a process for periodic review of the BCP's continuing suitability as well as timely updating of the document, specifically when there are changes in technology and processes, legal or business requirements;

- Develop a comprehensive BCP test approach that includes management, operational and technical testing;

- Implement a process of change management and appropriate version controls to facilitate maintainability;

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

- Document formal training approaches and raise awareness across the Commerce Department on the effect this might have on the auditee in the event of a disaster.

A DRP 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 the Commerce Department;

- 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 within the Commerce Department;

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

RECENT AUDIT REPORTS ISSUED BY THE NAO

NAO Work and Activities Report

January 2014	Work and Activities of the National Audit Office 2013

NAO Audit Reports

January 2014	Performance Audit: Addressing Social Benefit Fraud
February 2014	Information Technology Audit: Armed Forces Malta
March 2014	An Analysis of the Sourcing of Legal Services with respect to the Granting of Concessions to Operate Two Casinos
April 2014	An Analysis of WasteServ Malta Limited's Procurement: A Case Study Perspective
April 2014	An Assessment of the Macroeconomic Forecasts for the Maltese Economy Performed by the Ministry of Finance in April 2014
May 2014	An Assessment of the Main Fiscal Forecasts Prepared by the Ministry of Finance and Presented in the Update of the Stability Programme for Malta 2014-2017
June 2014	An Investigation into the Procurement of Legal Services by the Privatisation Unit between 2008 and 2013
July 2014	Performance Audit: Malta's Level of Preparedness to Deal with Oil Pollution at Sea
July 2014	Information Technology Audit: Employment & Training Corporation
October 2014	Foundation for Tomorrow's Schools: Regularity Audit on Procurement
October 2014	An Assessment of the Macroeconomic Forecasts for the Maltese Economy prepared by the Ministry for Finance in September 2014
November 2014	Performance Audit: Housing Authority's Procurement of Repair Works on Residential Units
November 2014	An Assessment of the Main Fiscal Forecasts
December 2014	Annual Audit Report of the Auditor General - Public Accounts 2013
December 2014	Annual Audit Report of the Auditor General - Local Government 2013