NAO
National Audit Office
MALTA

Information Technology Audit
Institute of Tourism Studies

Report by the Auditor General **July 2013**

Information Technology Audit

Institute of Tourism Studies
Malta

Table of Contents

List of Figures

List of Tables

List of Abbreviations

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

ADSL	Asymmetric digital subscriber line
BICS	British Institute of Cleaning Sciences
CCTV	Closed-Circuit Television
CD	Compact Disc
CdB	Common Database
CELT	Centre for e-learning technologies
CEO	Chief Executive Officer
CIMU	Central Information Management Unit
CIO	Chief Information Officer
CoBit	Control Objectives for Information and related Technology
CPU	Central processing unit
CSV	Comma-separated values file
DAS	Departmental Accounting System
DHCP	Dynamic Host Configuration Protocol
DOS	Denial of service
E-Mail	Electronic Mail
E-POS	Electronic Point of Sale
EU	European Union
FSS	Final Settlement System
GMICT	Government of Malta Information and Communication Technology
HR	Human Resources
ICT	Information and Communication Technology
IP	Internet Protocol
IT	Information Technology
ITS	Institute of Tourism Studies - Malta
LAN	Local Area Network
LSA	Learning Support Assistant
MAGNET	Malta Government Network
MITA	Malta Information Technology Agency
MLK	Martin Luther King
MOODLE	Modular Object-Oriented Dynamic Learning Environment

NAO	National Audit Office
NAS	Network attached storage
ODBC	Open Database Connectivity
OPERA PMS	OPERA Property Management System
OPM	Office of the Prime Minister
P2P	Peer to Peer
PABX	Private Automatic Branch eXchange
PC	Personal Computers
POS	Point of sale
SLA	Service level agreement
SMS	Short Message Service
SNMP	Simple Network Management Protocol
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
UUID	Universally unique identifier
VLAN	Virtual Local Area Network
WAN	Wide Area Network
Wi-Fi	Wireless fidelity

Executive Summary

Executive Summary

The National Audit Office (NAO) has conducted an Information Technology (IT) audit at the Institute of Tourism Studies (ITS) Malta. This audit sought to examine the Institute's IT operations, optimise the Institute's IT-enabled investments and 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 ITS - Malta has the necessary controls 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 related resources. Therefore, this report identifies potential risks and make recommendations to mitigate those risks.

Key Findings and Recommendations

The key issues addressed in this report (Chapter 2 refers) focused on how the ITS are managing their IT resources, in terms of hardware and software applications, network infrastructure and supplier management. The main findings and corresponding recommendations are listed below:

a. NAO noted that the IT Unit is run by two IT facilitators and therefore recommended that the unit should be headed by a qualified Head of IT. The Head of IT should extend the current IT operations to include IT management functions not just hardware support.

b. NAO found no evidence of a formalised IT Strategy for ITS and suggests that the ITS formulates an IT strategy through which it can ensure that the IT investment is not misdirected and draining resources which could otherwise be deployed differently.

c. NAO recommended that the ITS carries out a cost/benefit of its current IT and Information Systems investments.

d. In line with best practises, NAO recommended that ITS formalises its IT procurement process to include quotations, tenders and use of requisition forms.

e. NAO recommended that the Institute follows a formally structured and documented software project life cycle when building or procuring new software or enhancements on the existing software. This lifecycle should be implemented and managed by the IT Unit.

f. Currently ITS, does not have a local area network (LAN) infrastructure at Martin Luther King (MLK) building. NAO therefore suggested that senior management considers installing a LAN and a dedicated server in the MLK

building. Furthermore, NAO also recommended that the ITS should segregate the administration and the academia by connecting them on separate virtual local area networks (VLANs).

g. NAO suggested that the IT unit configures all the workstations so that these would log on the existing ITS domain and have a common set of relational security policies in place. Furthermore, ITS staff are to be made aware of the assigned network drives and the importance of using such drives when saving their data.

h. The NAO noted that the Wi-Fi system needed to be totally revised with the aim of increasing performance and reducing maintenance.

i. Following inspections at the Institute, NAO observed that the ITS servers were located in two different rooms; which required extensive changes so as to be considered as proper server rooms. NAO recommended that all servers are relocated into one room that is secure and adequate for this purpose.

j. NAO suggested that the IT unit carries out internal audits to verify authenticity of software applications and software licences on all existing personal computer's (PC), as part of its normal inventory process.

The IT audit reviewed nine software applications used within the ITS, the ITS website and the ITS facebook page (Chapter 3 refers), in terms of ease-of-use, the security controls in place, account management, hosting services, back-ups. The main findings and corresponding recommendations are listed below:

a. Some of the software applications currently in use at ITS are hosted on desktops rather than the central server. NAO therefore recommended that all software applications are:
   - hosted on the ITS servers and not on desktops;
   - backed up daily, back-ups are stored off-site, and test restores of back-ups are done periodically; and
   - administered and maintained by a system administrator.

b. NAO suggested that ITS carries out a BPR exercise aiming at reducing the current duplication of work. Examples of such duplication of work include: The concurrent use of an electronic and a manual stores system at the ITS Hardware Stores. Furthermore, invoices are currently being inputted three times by the accounts department, the inventory officer and the stores.

c. NAO recommended that ITS reviews whether the procured software application for inventory management purposes is still needed.

d. During the course of this audit NAO noted that certain software applications are being used by just one officer. NAO suggested that ITS trains multiple officers in operating each software application and thus removes any possible bottlenecks.

e. NAO observed that the e-learning system is only being used by about 50% of the lecturers and suggested that ITS establishes a training program for lecturers. NAO also proposed other solutions which senior management may opt for, so as to entice usage of this software application by both the students and the lecturers.

f. NAO reviewed the ITS website and recommended that this complies with the Government of Malta Information and Communication Technology (GMICT) standards. NAO also noted a number of broken links and recommended that these links are updated accordingly.

g. NAO also reviewed the ITS Facebook page and recommended that ITS appoints an officer in charge of maintaining this page. NAO noted that the "Welcome to ITS" page needs to be recreated and recommended that the contact information and the listed broken links are updated.

The report also includes a review of the Institute's IT operations (Chapter 4 refers) and recommended that:

a. ITS considers purchasing and implementing a centrally managed anti-virus solution.

b. All servers are backed up onto the Network Attached Storage (NAS) device and this device is either backed up on tape or mirrored onto a replica device.

c. ITS keeps back-up logs.

d. ITS set-up an off-site storage facility where the weekly and monthly tapes can be stored.

e. Government electronic mail (e-mail) accounts are provided to all the members of staff who require e-mail access.

f. ITS reviews its Wi-Fi network and ensures that:
   - Wi-Fi security is monitored and ensured at all times and in all parts of the building; and
   - it complies with the Government's Policy and directive vis-à-vis Wireless technology (GMICT Policy P 0047:2007 Wireless).

g. ITS implements an adequate web filtering solution on its Wi-Fi network through which gaming, video-on-demand and other bandwidth hungry sites are only allowed in certain parts of the building.

h. ITS holds a discussion with the Malta Information Technology Agency (MITA) to re-configure the government internet filtering package to address the Institute's needs.

i. All multi-function printers are connected to the internal network and stand-alone printers are phased out.

j. All servers are migrated into one server room that would be made adequate for the purpose. NAO also recommended that until this migration of servers is done, the annex room in which the e-learning server resides is cleaned from all clutter.

k. Physical security is improved in both the Institute's main building and the MLK premises.

l. ITS ensures that power sockets including the ones in the labs are not overloaded with extensions.

Chapter 5 of this report then documented aspects related to Information Security. In this regard, NAO suggested that a business impact analysis and a risk assessment exercise are carried out from which a business continuity plan is drafted.

The final chapter of this report lists the Management comments submitted by ITS. This report also documented the numerous corrective action initiatives that ITS Senior Management undertook during the course of this audit such as the immediate action taken to secure the Wi-Fi.

Chapter 1

Overview

Chapter 1 - Overview

The ITS was established in 1987 as an institution of higher education aimed at meeting the changing needs of the Hospitality and Tourism Industry.

The Institute aims to provide educational programmes in the field of Tourism. Furthermore, it seeks to identify and monitor customer needs and is responsible for providing the Hospitality Industry with personnel trained who can guarantee an excellent standard of products and services with the Industry.

In order to achieve these goals, the Institute:

- provides training in a comprehensive range of skills;
- develops and enhances the intellectual ability of its students through a wide range of academic subjects;
- teaches generic skills essential for a smooth transition into the world of work;
- recreates actual working environments on campus; and
- provides opportunities for work experience in the industry.

This document is a report issued by the IT Audits and Operations Section of the NAO covering the ITS (Malta) IT Audit exercise. It documents the current state of affairs at the ITS and provides an inventory of the technology and business processes associated with the ITS as it exists today.

Furthermore, it lists the findings that resulted from the Risk Based IT audit carried out and details the recommendations.

1.1 Background

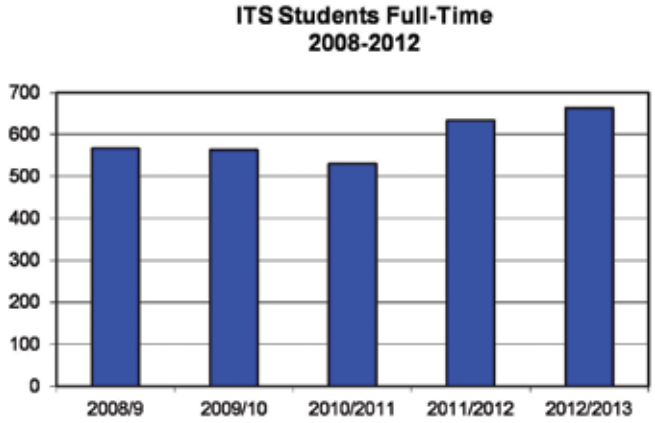
The ITS emphasises the importance of the relationship between the tourism, education and vocational training and offers further education programmes in this field.

As depicted in Figure 1 below, the ITS has increased the number of courses offered to its full-time students giving them the opportunity to get qualified in their specific areas.

Number of Courses offered	
Academic Year	ITS Full-Time
2008/9	18
2009/10	18
2010/11	17
2011/12	19
2012/13	20

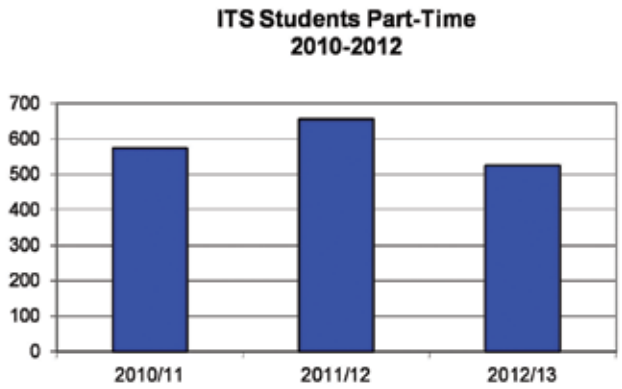
Figure 1: Number of courses offered

The ITS has also increased the number of both full time and part time students (Figure 2-3). As depicted in Figure 2 below, the number of full-time students has increased by 18% during the last four years.



Academic Year	ITS Students Full-Time
2008/9	568
2009/10	564
2010/11	531
2011/12	634
2012/13	664

Figure 2: ITS No. of Full-time Students



Academic Year	ITS Students Part-Time
2010/11	573
2011/12	656
2012/13	525

Figure 3: ITS No. of Part-time Students

The students graduating from the ITS has also increased by 12% during the last four years. Table 1 below, represents a breakdown of graduates at each level during the last four years.

Year	Level	Graduates
2008/9	Diploma	67
	Certificate	38
	Foundation	51
	ESTS	40
		196

Year	Level	Graduates
2010/1	Diploma	53
	Certificate	61
	Foundation	47
	ESTS	38
		199

Year	Level	Graduates
2009/10	Diploma	51
	Certificate	66
	Foundation	37
	ESTS	36
		190

Year	Level	Graduates
2011/2	Diploma & HND	61
	Certificate	108
	Foundation	27
	ESTS	23
		219

Table 1: ITS No. of Graduates

The ITS students following the Higher National Diploma and the Diploma Courses have a compulsory module that consists of an International Internship that would give the student a six month practical experience in the hospitality industry that are undertaken in a foreign country. Moreover, it is a module within the ITS Programme of Studies which carries 22 academic credits. Students have the opportunity to go for an internship in the following countries:

- Isle of Man
- England
- Ireland
- Scotland
- Belgium
- Czech Republic
- France
- Australia
- Spain
- Portugal
- Italy
- Netherlands
- Thailand
- Seychelles

The ITS' recent key achievements were:

1. New vision for the ITS (2010) –

   - Part 1: A Work Plan to increase the diversification of learning, and increase the learning opportunities for a diverse student body was devised. This plan is a strategy detailing the manner in which the ITS will continue to train quality workers in the tourism sector, including those who already work in the sector and need to improve their qualifications, position and salary. The vision of the ITS is also based on the strategy developed by the Government (Vision 2015) which recognises the tourism sector as one of the seven pillars of the country.

   - Part 2: Through this vision the ITS envisages to meet the increasing challenges of the industry and education in Malta, and plans to offer more learning opportunities for all, including vocational courses leading to a Bachelor's degree.

2. New Curriculum for the ITS (2011). Through this new curriculum the ITS restructured and increased its courses. Now the ITS offers nineteen qualifications out of which nine are at HND Level (MQF Level 5), six are at Diploma Level (MQF Level 4) and another four at Certificate and Foundation level (MQF Levels 2 and 3).

3. Legal Notice ITS (2012): In May 2012, the Government published a legal notice through which the ITS became an institution a greater level of autonomy. A new Board of Governors was setup under this law.

4. The ITS increased the number of students pursuing full-time courses as depicted in Figure 2.

5. The graduation in 2012, was the first one, from 2008 onwards during which, the number of graduates exceeded 200.

6. In October 2012, the ITS began courses for students with intellectual disabilities (Key Skills for Independent Living and Employment in the Hospitality Sector). The course focuses on consolidating the key competencies and skills required in Food and Beverage and Housekeeping Operations Sectors. This course is also helping these students in life skills that are important for independent living.

7. The ITS also has a large number of part-time students. The ITS is aiming to further improve its part-time prospectus so as to cater for the labour market demand.

8. During 2012, the ITS strengthened its management body and employed a number of lecturing staff. These include nine full-time teachers, 13 part-time teachers and one Learning Support Assistant (LSA).

9. In 2012, the ITS concluded the negotiations on a new collective agreement for teachers of the ITS. The new measures in this agreement included:

- introduction of a senior lecturer grade;
- increase in salaries, allowances and overtime rates;
- learning opportunities and professional development for teachers of the ITS; and
- more flexibility for teachers.

Recurrent Expenditure

The investment in the ITS has also increased by € 1.1 million from € 1.2 million in 2008 to € 2.3 million in 2013.

Capital Expenditure/Refurbishment costs

The ITS has also benefited from European (EU) funds. Table 2 below, lists the amount of EU funds and the amount of local co-financing funds, which the ITS has benefited from.

	European Funds	Local Funds Consolidated Fund	Total
Structural Funds 2008	€ 60,000	€ 21,000	€ 81,000

Table 2: European and Local Funds

The ITS has also made numerous improvements in its infrastructure and equipment. These improvements are financed through the yearly capital allocations made through the consolidated funds. Table 3 below details the capital allocations/expenditure in recent years.

	Budget - Consolidated Fund
Capital Allocation 2012	€ 45,000
Capital Allocation 2011	€ 45,000
Capital expenditure 2010	€ 44,999
Capital expenditure 2009*	€ 44,702
Capital expenditure 2008**	€ 46,997

Table 3: Capital allocations/expenditure

* In 2009, the ITS also benefited from € 29,000 EU Transition Facility
** In 2008, the ITS also benefited from € 1.6 million in Structural Funds 2004-2006 and € 298,271 in EU Transition Facility.
The ITS has invested the above funds in various projects, including the following:

- In 2009/10, the ITS established a cleaning laboratory (centre dedicated to Cleaning Science) in the MLK campus. The ITS is now an accredited training centre and a corporate member of the British Institute of Cleaning Sciences (BICS).

- In 2009/10, in collaboration with the Callebaut Brussels and their agents in Malta, the ITS launched a Chocolate Academy at the MLK campus.

In addition, the ITS is also using its funds for a series of improvements in its current campus:

- During the summer of 2011, the ITS has invested in a project of more than half a million (€ 500,000) to improve the student facilities, including the gymnasium, new food stores, two archive rooms, a room for the ITS security, laundry extension and other improvements on campus.

- During summer 2012, the ITS changed the floor tiles in its main restaurant (The Pembroke Suite). Furthermore, the ITS also carried out a refurbishment of the Vaults Restaurant with a total cost of € 39,180. The Vaults Restaurant is being used by advanced level students to gain experience in À la carte and experience in the innovation of cooking and catering services.

- The ITS is also building a new kitchen in its MLK campus. This kitchen will increase the amount of kitchen space and thus students will have added places to be utilised during kitchen individual sessions.

1.2 Organisation Structure

The ITS is presently composed of the units listed below:

- **Office of the Executive Director** - The Executive Director has the overall responsibility of managing the Institute including the management of the day-to-day operations of the Institute and the overall achievement of planned targets. Furthermore, the Executive Director is also responsible for the Strategic Development, the Marketing, the Public Relations and the industry liaison of the Institute.

- **Office of the Deputy Director** – The Deputy Director has the role of assisting the Executive Director and deputising in his absence. In addition the Deputy Director is also responsible of the Quality assurance.

- **Academic Studies Section** – This unit manages all matters relating to the curriculum, teaching, learning and assessment of the Institute. In line with the Government education policy and the needs of the industry, this unit is responsible for the development and the implementation of an adequate quality management procedures and systems, to ensure a smooth transmission of academic knowledge and other relevant skills to students. This unit is composed of subject co-ordinators, lecturing staff, guidance and counselling staff.

- **Office of the Registrar** – The Registrar manages the student management information system and the work placements of students. Furthermore, the registrar keeps the Institution's seal used upon certificates and awards, of which a full record is kept. Moreover, the registrar acts as secretary to the Board of Studies, ensures the proper safekeeping of the records of all examinations held by the Institute and keeps updated copies of the guidelines and procedures of the Institute. The Registrar also manages the administrative and organisational process of the learning activities of the students. Furthermore, the registrar keeps makes suitable arrangements for the learning timetable, upon consultation with the Board of Studies.

- **Administration** – This unit is responsible for managing the Finance section, the Human Resources (HR), the IT, the Inventory Management, the Institute's Library and the support services including the stores, housekeeping, maintenance, the drivers, the security and also the internal and external communications of the Institute. The Finance section is responsible for the accounts, asset management, financial controls, budgeting and communications with the Director of Corporate Services of the Ministry.

The ITS operates from two buildings, the main one in Prof. Walter Ganado Street St. George's Bay St. Julian's. The secondary Campus is the ex Martin Luther King Hall in Pembroke.

The ITS has a staff compliment of 146 employees, of which 117 are full-time, four are working on reduced hours, 22 are part-time and three are on a contract for service. As shown in Figure 4 below, most of the Institute's staff are administrative staff that include maintenance and housekeeping staff.

Category	Full time	Reduced Hours	Part time	Contract for Service	Total
Management	4				4
Academic Staff	42	1	21	2	66
Administration and Technical	71	3	1	1	76
				Total	146

Figure 4: Human Resources at the ITS

The organisation chart in **Annex A** depicts how the ITS is set up.

1.3 Legislation

The Institute carries out its functions under the Education Act (Chapter 327).

The Institute's functions are also regulated by Legal notice 131 and Legal notice 203 both issued in 2012.

The ITS is also regulated by the following:

- Legal Notice 294 of 2012 Malta Qualifications Framework for lifelong learning;
- Legal Notice 296 of 2012 Further and Higher Education. Licensing, accreditation and quality assurance;
- Public Administration Act Chapter 497;
- Financial Administration and Audit Act Chapter 174; and
- Public procurement regulations.

1.4 ICT at the Institute of Tourism Studies

1.4.1 Applications

The IT Systems used at the ITS are:

- **SITS: Vision** – SITS is a student records management system used to store, administer and manage all aspects of student information from initial enquiry and application through to course admittance and course completion.
- **Students minor offences logging system** – a software application developed in house to record students minor offences.
- **HQ Horizon Food and Drink Edition** - used as an epos billing system at the Pembroke Restaurant, the Vaults Restaurant and the Palms Cafeteria.
- **Intact Business Management System** – procured so as to be used for Inventory Management purposes.
- **Library - WiSDoM 4** – used by the Library to keep track of all the books loans and the books at the library.
- **Hardware Stores - WiSDoM 4** - is a stock control system used at the Hardware Stores.
- **Food and Beverage Manager System** – is a stock control system used at Food Stores Department.

- **Departmental Accounting System (DAS)** – The DAS, which the Maltese Government uses for financial management.

- **Common Database online query (CdB)** - The CdB is a central data repository used by Government entities to access information about persons, addresses, organisations and the inter-relationships between these subjects.

- **Fleet management System** – used to issue and keep track of fuel chits for ITS vehicles.

- **E-learning** - a system built in house through which the students and lecturers have a virtual platform where class notes, learning material including videos and recordings, tests, homework, grades, assessments are uploaded.

- **OPERA Property Management System** – a property management system used by the hotel industry for reservations, billing etc. This system is being used by the ITS for lecturing purposes.

- **Dakar Payroll** – a Payroll system that provides complete payroll processing of all the employees. This includes the maintenance of the Institute's employee details, the management of leave, actual payroll calculation, printing of payroll reports and payslips, processing of direct credit payment and submission of periodical Final Settlement System (FSS) returns as required by the current legislation.

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

- SITS: Vision;
- Student Minor Offences Logging System;
- HQ Horizon Food and Drink Edition;
- Intact Business Management Software;
- Library - WiSDoM 4;
- Hardware Stores - WiSDoM 4;
- Food and Beverage Manager System;
- E-learning; and
- OPERA Property Management System.

NAO will also review the ITS website and the ITS Facebook page.

1.4.2 IT Labs and Infrastructure

The ITS has five labs in its St. Julian's building and one lab at MLK as detailed hereunder:

- Room 227 – a lab comprising of an interactive white board and of 20 PC's, each with a Wi-Fi dongle.
- Room 103 – a lab comprising of an overhead projector and 12 PC's, each with a Wi-Fi dongle. MITA connectivity is also available in this lab.
- Room 102 – a lab comprising of an overhead projector and of 20 PC's, each with a Wi-Fi dongle. MITA connectivity is also available in this lab.
- Room 101 - comprising of nine PC's connected to the government network. No Wi-Fi connectivity is available in this lab.
- Resource Centre – comprising of 12 PC's, each with a Wi-Fi dongle.
- Room 618 (MLK) – a lab comprising of 20 PC's, each with a Wi-Fi dongle.

The ICT Infrastructure at the ITS consists of:

- **Servers and Storage Hardware** - The Institute has six servers, 3 of which are virtual machines, and a Network Attached Storage (NAS).
- **Personal Computers** - The PC's are procured by the ITS.
- **LAN Network** – The LAN is supported by the ITS. An Asymmetric Digital Subscriber Line (ADSL) line connects the Institute to Malta Government Network known as MAGNET. This LAN is only available at the Institute's main premises in St. Julian's.
- **Wi-Fi Network** – The ITS has a Wi-Fi network at both its sites. The Wi-Fi is used by students, lecturers and administrative staff and is administered by a third party supplier.
- **E-mail System** - The Institute uses MITA's e-mail system.
- **Office Automation Software** – Office Automation software licenses are purchased by the ITS.
- **Telephone System** – A Private Automatic Branch eXchange (PABX) is in place.

For the purpose of this audit, NAO will be reviewing the management and maintenance of the above listed infrastructure.

1.5 Audit Scope and Objectives

The scope of this engagement was to analyse the IT and the Information Systems used by the ITS, identify any potential risks and make recommendations to mitigate those risks.

The IT Audit carried out consisted of three different stages:

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

- The Institute's overall strategic direction, objectives, internal structures, functions and processes were then studied in order to gain a comprehensive understanding of the organisation and its environment. This included in-depth interviews with key officials and stakeholders, as well as observations and a review of documentation.

- The third stage involved examining the manner in which the Institute uses its IT investments, the user friendliness, maintenance and security of its IT systems, the business continuity and disaster recovery measures adopted and the supplier management. This audit also looked at workflow management to evaluate the processes and procedures involved so as to recommend how these may be improved in terms of increasing efficiency and reducing any possible errors.

Therefore, the objectives of this report were to:

- document all the information collected during the numerous interviews held with various officials;

- summarise the documentation collected and elicit the area/s of concern;

- determine whether the ITS' IT systems operate effectively, efficiently and economically;

- record the findings and identified related risks; and

- list the recommendations.

1.6 Audit Methodology

In order to attain the above objectives a number of interviews were held with a number of officials at the ITS.

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

1.7 Structure of the Report

The report includes five further chapters, each documenting the information collected and highlighting the findings and recommendations with reference to particular aspects of this audit:

- Chapter 2 deals with the IT management perspective and analyses the procedures of the IT unit evaluating the manner in which ICT resources are managed.
- Chapter 3 reviews the ITS' suite of software applications in greater detail.
- Chapter 4 evaluates the IT operations of the Institute including the Institute's use of social media, and assesses the IT risk management, business continuity and disaster recovery.
- Chapter 5 assesses the Information Security and evaluates the security measures adopted by the Institute to maintain the confidentiality, integrity and availability of data.
- Chapter 6 lists the management comments.

1.8 Acknowledgements

NAO would like to express its appreciation to all the staff within the ITS, who were involved in this audit, particularly the Executive Director, the Head of Accounts, the Head of Administration and the IT Facilitators for their time and assistance.

Chapter 2

Information Technology Management

Chapter 2 - Information Technology Management

2.1 Information Technology Unit

The ITS has two IT Facilitators one of whom was appointed in 2004 to co-ordinate projects and provide technical support. The other IT Facilitator was allocated to the IT Section in 2011.

In NAO's view the functions of the IT unit should not be dependent solely on two IT Facilitators. NAO recommends that such a unit should be headed by a qualified Head of IT who would be made responsible for all the IT projects and IT administration. NAO observed that currently the IT unit is only handling hardware support and recommends that the functions of this unit include:

a. Policy and management, which would cover:
   - developing and implementing organisation wide IT policies;
   - contingency planning and disaster recovery;
   - project management;
   - procurement of IT equipment, systems and services; and
   - management of suppliers and contractors.

b. Provision, service and maintenance of Infrastructure, which will cover:
   - computers, printers, and other hardware;
   - operating systems and standard productivity software;
   - networks, LANs and WANs and servers;
   - connectivity;
   - telephony and PABX systems; and
   - power back-up.

c. Applications and Information Systems which would cover:
   - management of suppliers, providing enhancements and upgrades;
   - call-logging of all calls forwarded to suppliers;
   - user Training;
   - back-ups;
   - account Maintenance including creation and termination of logins;
   - audit trail management;
   - updated to the ITS Website and Facebook page; and
   - report Generation.

d. Help Desk and User Support.

e. Management of all labs both at the ITS St. Julian's and at MLK.

f. Establishing communication with all external suppliers that are providing IT services to the ITS. All requests for maintenance to IT systems and hardware should be channelled through the IT Unit and the IT Unit should keep a log of all calls and requests forwarded to IT suppliers, detailing the date when the call was opened, the type of call, the action taken by the ITS, the action taken by the supplier concerned and the date when each call was closed. Call logging may also be analysed from time to time so as to help management in decision making and future planning.

g. Establishing a working relationship with the Ministry's Chief Information Officer (CIO) office. Such relationship can help the ITS in implementing its IT initiatives and goals.

Although the Institute's IT requirements are sometimes discussed in ad-hoc meetings. NAO suggests that regular meetings are scheduled and held between the IT unit and management so as to discuss the ongoing IT requirements, provide feedback on ongoing IT projects and discuss any improvements to IT operations. NAO noted that, during 2012, two IT meetings were held.

2.2 ICT Strategy

An ICT Strategy is a comprehensive plan consisting of objectives, principles and tactics relating to the use of ICT technology in an organisation. The ICT strategy is intended to express how technology is to be utilised so as to achieve the goals of that particular organisation in line with its business strategy.

Nowadays ICT is not just an enabler but can also be considered as a driver and thus an organisation should have an ICT Strategy so as to ensure that the money being spent of ICT is being used to the best effect to further the organisation's strategic aims.

An ICT Strategy is essential to ensure that all ICT development projects form part of an overall plan and prevent a 'laissez faire mushroom' approach which leads to fragmented ICT development without the required central control and planning. Furthermore, NAO considers that an ICT Strategy is especially essential for organisations like the ITS where resources are limited and one needs to derive the maximum value from its ICT investment.

The ITS does not have a formally documented IT strategy and therefore NAO suggests that the ITS formulates a strategy that:

- makes reference to the IT and Information Systems projects and explains how these projects are linked to the ITS Business Strategy, and how these projects are going to be implemented;
- prioritises future ICT investment;
- covers the development being planned in the next three to five years; and
- refers to the Logical and Physical architecture of the ITS IT systems.

Through this ICT strategy, management can gauge whether IT is delivering strategically and can ensure that the IT investment is not misdirected and draining resources which could otherwise be deployed differently, to the benefit of the organisation.

The IT Strategy document may be compiled by the Head of IT in close collaboration with the ITS Senior management and with the Ministry's CIO office. Furthermore, this strategy must be kept up to date and changed in response to new organisational circumstances or business priorities, budgetary constraints, available skill sets, core competencies, new technologies and a growing understanding of user needs and business objectives.

2.3 ICT Budget

During the course of this audit, NAO reviewed the actual ICT capital and recurrent expenditure of the ITS in 2012 and that planned for 2013.

ICT Expenditure	
2012	€ 109,604
2013 (planned)	€ 170,000

Table 4: ICT Expenditure

NAO noted that as depicted in Table 4 above, the planned ICT expenditure for 2013 is 55% higher than that for 2012, however this is due to a planned investment in a new Accounting, HR and Payroll Package.

NAO also noted that the services being provided by MITA are covered by a Ministry contract (as detailed in Section 2.5) and thus are not included in the above quoted ICT expenditure figures.

Furthermore, NAO observed that although the actual expenditure for 2012 was € 109,604 the allocated funds for IT in 2012 were €98,000 and thus there was an overrun of € 11,604.

During the course of this audit, NAO also reviewed the percentage of IT funds being spent on new IT investment and compared it with the percentage of funds being allocated towards IT support. As depicted in Table 5 below, NAO noted that the majority of IT expenditure is being allocated towards new IT investment.

	2012 (actual)	2013 (planned)
IT Investment	85%	86%
IT Support	15%	14%

Table 5: Break down of IT Expenditure

NAO recommends that as a best practice, the ITS carries out an exercise to analyse the cost/benefit of its IT and Information Systems. This exercise can be done by the Head of IT and the Head of Accounts conjointly and the results should then be passed on to senior management. Through this exercise senior management can ensure that IT expenditure, including the cost of software licenses, is justified.

2.4 Project Life Cycle

NAO deems project management as a very important function and has thus reviewed the ITS' project life cycle, both in terms of Hardware and Software. NAO reviewed the processes involved in procurement, maintenance and disposal of hardware equipment and the planning, development, acquisition, testing, implementation and maintenance of software applications.

2.4.1 Hardware project life cycle

Procurement

The ITS opted not to join the Government's PC leasing scheme and thus procures all its IT hardware including computers, laptops, printers, photocopiers, scanners, projectors, servers, routers, switches etc. The procurement process is generally kicked off with a verbal request from the IT unit or from senior management to the Head of Accounts. The Head of Accounts then gathers quotations for the items required and the successful supplier is selected. The necessary approvals are then obtained from senior management and the items required are procured.

NAO recommends that as a best practice, the ITS should formalise its procurement process and implement a system whereby a requisition form is filled in, for the IT hardware required. This requisition should then be passed on to the Head of IT who, after obtaining the necessary approvals, obtains quotations or issues a tender depending on the cost of the items being procured. The Head of IT should then analyse all the quotations received and pass on them on to senior management together with technical recommendations. Senior management would then take the final decision.

Maintenance

NAO noted that at the ITS, hardware maintenance is done by the IT facilitators who contact the suppliers when an item is still under warranty or when the incident cannot be resolved by them.

NAO suggests that a log of all calls for maintenance is kept so as to be able to detect any defective equipment, problematic suppliers or calls of a particular nature, which collectively may indicate a common source. Such information can also help in decision making.

Disposal

During the course of the audit NAO enquired about the disposal procedure adopted by the ITS for IT hardware which is either obsolete or beyond repair. NAO was informed that from time to time a board is formed so as to decide which hardware is to be disposed of, and this is done accordingly. NAO was also informed that the board keeps record of all hardware being disposed of, although a copy of such records was not given to NAO.

NAO recommends that the ITS ensures that all boards formed, to survey the disposal of hardware, submit a list of all equipment being disposed off to senior management and all lists are kept in one central place. The board should also be responsible to submit a copy of such lists to the Head of Accounts and to the person in charge of the Inventory. Furthermore, NAO recommends that such lists include the details below:

- Date of survey.
- Members on the board of survey.
- Item Inventory Number.
- Item Serial Number.
- Item Description.
- Reason for disposal (Ex. Certified beyond economical repair, certified obsolete).

Moreover, NAO recommends that when a technician certifies hardware as beyond economical repair or obsolete, this certification is done in writing and handed to the board of survey together with the item in question. Such certifications are to be attached to the board of survey's final disposal report.

NAO also enquired about the procedure adopted by the ITS when disposing of hard disks or other hardware that may contain data. NAO was informed that the IT facilitator formats such hardware prior to putting it aside for disposal. Although this initiative is a good first step, NAO recommends that the Institute adopts the Desktop Services Procedure (GMICT R 0084:2009[1] in terms of PC Disposal and Data Wiping, so as to ensure that data may not be retrieved by any third party.

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

NAO suggests that the IT facilitator, when disposing of hard disks or other hardware that may contain data, inserts a note documenting the date when the data was wiped and by whom. This note could be done on the form certifying the item obsolete or beyond economical repair. By doing so the board certifying the item for disposal can ensure that the data wiping procedure was carried out.

2.4.2 Software project life cycle

During the course of this audit, NAO reviewed the manner in which the ITS approaches software development projects and the manner in which off-the shelf software is procured. NAO observed that at the ITS there was no evidence of a structured, systematic way of building or procuring software applications. The consequence of such a situation is that certain software:

- does not match the internal business process;
- was procured but not utilised;
- is not being utilised to its full potential;
- is causing duplication of work; and
- does not meet the need of the end user.

Furthermore, NAO observed that the procurement and development of software, is not being managed by the IT unit but only by the end user and senior management. Although senior management is the final decision maker when procuring new software, NAO recommends that this should be done as part of a software project life cycle implemented and managed by the IT Unit. NAO thus recommends that the Institute follows a formally structured and documented software project life cycle when building or procuring new software and when enhancements to software are made.

The Software project life cycle implemented should include the six phases mentioned 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.
- **Maintenance phase** - Maintaining the software throughout its lifetime.

Annex C contains a template detailing the questions to be answered during each of the above stages.

Moreover, NAO suggests that a business process re-engineering exercise is carried out through which the ITS studies how it can meet the end users needs and identify solutions as to how the current software can be enhanced with the aim of minimising the duplication of work and ensuring that this software meets the current requirements. NAO recommends that the IT unit takes an active role in this regard and provide management with the necessary technical advice needed.

2.5 Third Party Suppliers

The ITS has entrusted MITA, being the ICT Agency for the Government of Malta, with the provision of e-mail and internet services. MITA provides the ITS with an ADSL connection to the MAGNET and provides 24x7 monitoring of this connection.

Furthermore, MITA is providing the ITS with access to MITA's service call centre and first line support for the reporting and resolution of incidents regarding e-mail and internet.

During the course of this audit, NAO observed that MITA related services are covered by a Ministry contract. NAO recommends that the services are covered by a specific contract between MITA and ITS. A subvention from the related ministerial budget can be made in this regard.

The ITS however has various service and maintenance contracts with other suppliers. NAO reviewed these contracts and agreements and recommends that the ITS ensures that these contain suitable Data Protection Clauses.

Moreover, NAO was not provided with copies of contracts or agreements covering website hosting and maintenance. The ITS, should ensure that maintenance contracts are drafted for all services being acquired from third parties.

2.6 Network Infrastructure

The ITS' main building in St. Julian's, is connected to the Government Network generally referred to as MAGNET, via an ADSL connection to MITA. Network connectivity is monitored and maintained by MITA on a 24/7 basis.

2.6.1 Local Area Network and Wide Area Network

Internally the ITS (St. Julian's) operates a LAN based on one gigabit Ethernet switches. Each switch has a fibre optic backbone. The ITS LAN is supported by the IT Unit. NAO recommends that the IT unit takes a more proactive role and monitors the LAN so as to check for outages of network devices, monitor network performance and usage of network resources.

The MLK building is not connected to the Government Network and third party internet services are provided through a Wi-Fi system. Furthermore, NAO observed that this building did not have a LAN. In the absence of a LAN the lecturers needing to print any material are expected to save on a pendrive and then access the contents on the pendrive from the PC at the reception desk to print the material required on a stand-alone printer connected to this PC. Moreover, due to the absence of a LAN server, ITS staff at MLK can only save their data on their desktop risking data loss if a hard disk malfunctions.

As pointed out in Section 4.7, NAO noted that at MLK, there is a multi-function networkable printer/scanner which is not connected to a pc and is only used for photocopying purposes. NAO suggests that senior management considers installing a LAN and a dedicated server in this building, especially if it intends extending the use of this campus. The existing multi-function printer can then be connected to this LAN so as to make better use of it.

As part of this audit, NAO requested a network topology diagram of both the ITS LAN and Wide Area Network (WAN) however these were not available. NAO recommends that the above diagrams are obtained or drafted and proper labelling is in place.

NAO also recommends that the ITS should segregate the administration and the academia by connecting them on separate VLANs, thus minimising the risk of any possible viruses/malware from proliferating through both sections.

NAO observed that not all networking equipment is connected to an Uninterrupted Power Supply (UPS). NAO suggests that each device is connected to a UPS that incorporates a network management card. The aim of the network management card is to provide a secure monitoring and control of the UPS via a web browser. The network management card will then be configured to send an e-mail notification to the server administrator in the event of a power disruption. UPS' should also be regularly tested by the IT Unit. A log of these tests should be kept.

NAO recommends that the ITS invests in an availability and monitoring solution, that apart from checking whether a device is online or not, it will also monitor performance indicators such as the Central Processing Unit (CPU), memory, network, disk space and processes on all servers. The system must cater for both Windows and Unix based systems and should be able to monitor devices that support SNMP (Simple Network Management Protocol), through which anything from CPU performance of the monitored device, temperature, memory usage and uptime could be monitored. This system will alert the network administrator immediately if for example a particular lab does not have network connectivity rather than awaiting for such a problem to be discovered by a lecturer whilst giving a lesson.

Apart from implementing the above mentioned solution, NAO recommends that the ITS or its suppliers configure every device (that can be configurable) to send an e-mail to a specific mailbox or set of mailboxes or through Short Message Service (SMS), for every critical alert, in order to rectify the problem in the shortest time possible. These alerts could vary from power failures, to server CPUs/memory high usage, low disk space etc.

In order for the ITS to choose a monitoring software that best suits their needs, one must consider specific criteria, namely: scalability, ease of used, reactive monitoring and total cost of ownership. There are several monitoring software solutions that the ITS could consider, some of which are even open source.

During the course of this audit, NAO noted that all workstations at the ITS are set up using a workgroup model which is generally use for home and small business environments and through which security policies can only be assigned and enforced locally by configuring them on each and every workstation. Apart from being time consuming, this setup has a number of disadvantages including that the username and password must be set on each and every workstation.

NAO observed that the ITS however has all the infrastructure in place to migrate to an Active Directory domain model. Consequently, NAO suggests that the IT unit configures all the workstations so that these would log on the existing ITS domain and have a common set of relational security policies in place. By using a domain, the IT Unit would create a single platform to manage the whole network and also be able to:

- control the level of access a user has to resources;
- roll out software automatically;
- apply global settings to all users via Active Directory;
- use Group Policies to centrally manage and configure operating systems, applications, and users' settings;
- use logon scripts to assign tasks that will be performed when a user logs on to a particular computer. These scripts can also carry out operating system commands, set system environment variables, and call other scripts or executable programs;

- offer a greater level of flexibility to its users, since a user can login on any computer in the network and access his/her resources. This would effectively allow users to work from any computer on the network as Universally Unique Identifier's (UUID) are synchronised with Active Directory;

- improve workstation security. Computer policies can be set by IT Unit to automatically update and secure workstations through group policies;

- reduce overhead through standardisation;

- allow the sharing of resources such as files and printers. This would enable teams or sections to share files and resources without having to create local user accounts for sharing;

- allow users to use Home and Departmental network drives for their office automation files, which in turn will be backed up on a daily basis as recommended in Section 4.3 of this report; and

- allows the administrator to make changes faster and improve functionality without requiring user intervention to invoke changes.

Furthermore, NAO suggests that all ITS staff are made aware of the assigned network drives and the importance of using such drives when saving their data. NAO observed that currently several users are saving their data on the local workstation risking to lose everything if a hard disk failure occurs. The IT unit may issue a memo or circulate an e-mail so to increase awareness in this regard.

The IT unit must also ensure that all network drives are backed up daily as detailed in Section 4.3 of this report.

Moreover, the IT unit must ensure that all the software applications used by ITS are hosted on a server. As detailed in Chapter 3, NAO noted that some software applications are hosted on particular workstations. Back-ups of these systems are not generated automatically but are taken by users from time to time. NAO urges the IT unit to rectify this situation immediately to avoid the risk of losing all the data.

2.6.2 Wi-Fi Infrastructure

The ITS has a 30 Megabit Internet and Wi-Fi connection which is being maintained by a third party supplier.

NAO noted that the Wi-Fi system at the ITS was implemented by connecting all routers in series (daisy chaining). Although such a system is working, the network is slow and users are facing performance issues. NAO noted that the IT unit installed a timer with each router to automatically switch it off and back on again. This was done so as to avoid the problem of having to reset routers.

NAO suggests that this setup is totally revised with the aim of implementing a more efficient set up that would require less maintenance and provides all users with a better connection.

2.6.3 ITS Server room

NAO also held site inspections in the Institute's server room and observed that this room is equipped with a fire alarm sensor and a carbon dioxide fire extinguisher which was serviced regularly by the supplier. Furthermore, NAO observed that the server room is kept locked and a log of all people requesting the keys is kept.

During these site inspections NAO also noted that the network cabinets were open, the air-conditioning unit was switched off awaiting repair and there was a fitted carpet. Moreover, NAO was informed that the room was equipped with curtains however these were removed as the air-conditioning unit was leaking.

NAO also noted that the e-learning server and the server being used for the Wi-Fi systems were not in the server room but were placed in an annex to the classroom of the IT lecturer. NAO observed that this room was very cluttered, did not have a fire sensor installed and power sockets were overloaded with extensions creating a fire hazard. This room was accessed by the IT unit, the IT lecturer who maintains the E-learning server and the third party supplier who supports the Wi-Fi system.

NAO recommends that the ITS re-locates all the servers into one room. Furthermore, NAO recommends that such room:

- is fitted with an air-conditioning system which is kept on at all times;
- is kept under lock and key and a log is kept of who accessed the room with the date and time;
- has no curtains, fitted carpets and other fire hazards;
- is equipped with an adequate fire extinguisher that is serviced regularly;
- is equipped with a fire alarm sensor;
- is kept clean and free from clutter;
- is located in a secure part of the building. i.e. any windows should lock securely and iron bars should be installed if windows are easily accessible;
- all cabling in this room is labelled and is passed through proper trunking. Furthermore, all cabling should be organised in an orderly fashion that is manageable and that fits well in the network cabinet; and
- is equipped with a humidity/temperature monitor that sends alerts via email/sms if it reaches a pre-defined threshold.

NAO acknowledges that the Wi-Fi system may need to be reviewed as the manner in which it was originally implemented may be problematic when considering server re-location.

2.7 IT Inventories

NAO acknowledges that one of the toughest tasks of IT managers and administrators is keeping track of computers, network devices and software. However, this is considered to be a very important exercise since through such information, the Institute would be in a position to keep track of its IT investments and be able to manage these resources as efficiently as possible.

NAO noted that the IT unit at the ITS does not keep an IT inventory but the ITS has an inventory officer who keeps an inventory of all physical items on a spreadsheet. NAO observed that this inventory was very comprehensive and included all IT hardware together with the asset number, the date when the item was acquired, the location and the cost.

During the course of this audit NAO has however observed a lack of control on Wi-Fi dongles which are also not listed in the inventory. NAO observed that some lecturers carry the Wi-Fi dongle with them at home and Wi-Fi dongles at MLK are sometimes disconnected and kept by the messenger to avoid having them stolen. NAO suggests that Wi-Fi dongles are to be included in the inventory, and management should issue a memo with a clear way forward as to whether these dongles are to be disconnected from the PC's and if yes, designating a central place where these dongles are kept in a controlled manner when not in use.

Furthermore, NAO noted that although a computer lab (Room 618) at MLK comprising of 20 PC's was turned into a classroom with all the PC's being stored away, the inventory spreadsheet still listed 11 PC's in this particular room. NAO thus suggests that a review of this inventory list is done so as to ascertain its accuracy.

NAO recommends that as a best practice, this list should be stored on the server and be accessible to the IT unit.

Furthermore, NAO suggests that the IT unit carries out an internal audit to verify all PC's in terms of authenticity of software applications and software licences. As a result of this audit the IT unit should compile an inventory of software applications and licences and amalgamate this with the original inventory.

Chapter 3

Information Technology Applications

Chapter 3 - Information Technology Applications

3.1 Software Applications

3.1.1 SITS: Vision

The SITS: Vision software is an off-the-shelf Student Management System that manages student administrative processes from course enquiries through to graduation. SITS was produced by a UK company, namely Strategic Information Technology Services Ltd (SITS) which was then acquired by Tribal Group plc in October 2004. The software which is used by around 75 universities and colleges across the UK, is subdivided into functional areas each of which is further subdivided into functional components that can be purchased separately according to entity's needs.

NAO noted that the ITS purchased the use of the below components:

- **MenuSystem** (MENSYS)
  - User Facilities
  - Menu Supervisor
  - Award Certificate Production

- **Marketing and Admissions System** (MAS)
  - Enquiries and Admissions

- **Student Registration System** (SRS)
  - Student Registration
  - Student Course Assessment
  - Fees and Invoicing
  - Student Placements

- **Modular Scheme Management** (MSM)
  - Scheme Definition
  - Student Scheduling
  - Programme Planning
  - Module Assessment
  - Management Information
  - Attendance Recording
  - Exam Scheduling
  - Module Timetabling

The ITS uses the SITS: Vision to input all courses of study and their related modules. Furthermore, the ITS also inputs records related to lecturers, classes, labs and kitchen.

The SITS: Vision is also used to input all applications for courses from prospective students. Each application form is then reviewed and the ones accepted are flagged in the system. The SITS: Vision then enables ITS to transfer the electronic record of prospective students to current student records. Each student record is linked to a course of study with a specified modules and the related lecturer for those modules. i.e. Student records in the SITS: Vision start with a record of a prospective student applying to a course but are then automatically updated through the various stages to hold all of a student's personal details. A student record will thus remain with the student for the whole of his/her studies at the Institute.

Through the SITS: Vision, ITS also issues student and lecturer timetables together with schedules of class, lab and kitchen use. The SITS: Vision thus enables ITS to monitor the use of its resources and maximise the potential of its kitchens, labs and classrooms.

The SITS: Vision is also used to automatically compile and issue timetables of all exams and resits. Furthermore, all exam results are inputted in the SITS: Vision.

During the course of this audit NAO noted that the version of SITS: Vision used by the ITS is an old 2001 version which is no longer supported by the supplier. NAO was however informed that notwithstanding this notification Tribal UK were still supporting ITS. In view of the above situation, NAO recommends that ITS should re-assess the deliverables listed on the support agreement.

NAO also noted that ITS has a knowledgeable officer who operates this system and takes care of all the account management and user management of this system. This officer has also linked the SITS: Vision Report Generator through Open Database Connectivity (ODBC) to Microsoft Access database and extracts all the data required to build custom reports and to integrate this system with the Students Minor Offences Logging system (Refer to Section 3.1.2).

NAO observed that the users of this system were given hands on training but are supported by the officer in charge who guides them accordingly with any day to day difficulties. NAO also noted that although ITS do not have any physical hard copy user manuals of this system, the SITS: Vision has a very comprehensive online help facility that even includes forums. Furthermore, the officer in charge informed NAO that the supplier also offers support through email/phone and generally any issues are solved within the day through remote access. However, the application loads an error, stating "System move aborted" when exam timetables are amended and particular exams are re-scheduled to a different time/date. NAO noted that this bug was reported to the supplier but ITS opted for a workaround that entails moving all

records involved one by one. NAO notes that although this solution is time consuming and is subject to human error, it is albeit a workable solution.

NAO also noted that the version of SITS: Vision currently being used by ITS does not have a facility through which it can send notifications to students via SMS. Moreover, NAO noted that student attendance is currently being inputted manually in SITS, since the current version being used by ITS does not have a facility through which this can be done electronically by lecturers. Upon discussing this with management, NAO was informed that ITS management is currently reviewing the options available and NAO recommends that the option should follow a software project life cycle as detailed in Section 2.4.2 of this report.

During the course of this audit NAO also reviewed the security of this application and noted that the application has a facility through which the administrator assigns different user rights and difference access levels i.e. when creating/amending a user account the administrator has the facility to grant access to particular screens of the software application and give view/read/write rights on each of these screens as applicable to that particular user.

NAO also noted that the SITS: Vision has audit trails and functionality related to password complexity and expiry but these are currently disabled. NAO was informed that since this application was being used by less than ten people ITS never felt the need to enable such functions. However, NAO is of the opinion that an entity cannot wait for a security incident to occur prior enabling such security functions and thus recommends that the ITS enables the audit trails, the password complexity and the password expiry functions on this application. NAO also noted that logins of past employees are still showing on the system and thus recommends that these are removed.

As part of the audit, NAO enquired about the back-ups/restore procedure for this application. NAO noted that although this application is hosted on ITS main server and is thus being backed up daily, ITS has never tested these back-ups and does not have an off-site storage of back-ups. NAO recommends that the ITS periodically performs a test restore of these back-ups so as to ensure that this can be done successfully should a disaster occur. NAO also recommends that an off-site facility of back-ups is available as recommended in Section 4.3 of this report.

3.1.2 Student Minor Offences Logging System

The Student Minor Offences Logging System is a custom built, Microsoft Access database application implemented in 2012, to record minor offences of ITS' students.

NAO noted that this system was an in-house custom built software application and is linked through ODBC with SITS: Vision tables so as to obtain student data. This system was implemented at the registry to keep an electronic record of minor offences and facilitate the registry's daily work. Minor offences are recorded on a manual form by lecturers and handed over to the registry where they are inputted in this system. The system then automatically flags students with three or more warnings and issues a report accordingly. Management is then alerted and the above mentioned students are then given a formal verbal warning.

This system is being used by one user and has no login/password. NAO recommends that such an application is enhanced with a login/password framework and an audit trail that records all transactions inputted in this system.

During the course of this audit NAO noted that this application is hosted on a shared folder on ITS main server and thus is being backed up daily. As recommended earlier in Section 3.1.1 NAO recommends that ITS should perform a periodic test restore of back-ups so as to ensure that should an incident occur the data in this application could be restored from back-ups. NAO also recommends that an off-site storage of back-ups is available as per Section 4.3 of this report.

3.1.3 HQ Horizon Food and Drink Edition

The ITS has three catering establishments namely the Pembroke Restaurant, the Vaults Restaurant and the Palms Cafeteria. Each catering establishment serves a variety of items and thus has a different menu. Furthermore, each catering establishment is equipped with a touch-screen Point of Sale (POS) terminal and use the HQ Horizon Food and Drink for billing purposes.

The HQ Horizon is an Electronic Point of Sale (E-POS) software application developed by HQ Soft S.r.l. that is represented in Malta by a local supplier. As depicted in Figure 5, the screen-interface is tailor-made for each of the above mentioned outlets to cater for their different menu items. The software application used by each outlet is integrated with a backend system that is accessed by the accounts department to oversee the collection of revenue and generate monthly management and tax reports. The E-POS systems also have the facility to issue x-reads (that read the sales totals), z-reads (that reset the sales totals) and end of day reports.

NAO observed that the ITS uses these systems to teach its students how to operate an outlet and how to act as the cashier during each practice session. NAO also observed that the students use the login account of the lecturer, however this is only done since it is not practical to create an account for each student. Furthermore, the student is logged in to the system by the lecturer who delegates the cashier duties to him/her. The lecturer remains ultimately responsible of all the revenue collected during the session. NAO noted that the cash reconciliation sheet that is completed at the end of each session is signed by the student acting as the cashier for audit trail purposes.

NAO noted that the management of user accounts, maintenance and enhancements are carried out by the third-party supplier. NAO observed that E-POS terminals are still displaying login accounts of ex-lecturers. NAO recommends that the supplier is instructed to terminate this access.

The ITS also depends on the supplier to carry out a simple price or menu change. However, NAO was informed that although there is no Service Level Agreement (SLA) with the supplier, the requests were serviced in a timely manner and most of the requests are serviced within the day.

During the course of this audit, NAO noted that when a lecturer is supervising a lunch and a dinner practice session at the same restaurant, he/she is unable to issue an end-

of-day report listing the lunch transactions and the dinner transactions separately. In this regard, the lecturer is not in a position to distinguish between the total cash in hand with the sum of all the transactions listed in the end of day report. NAO therefore suggests that apart from an end of day report this system issues an end of session report.

Furthermore, NAO noted that the system does not issue any other reports apart from the one mentioned above. NAO observed that lecturers are currently compiling some reports manually and would thus recommend that management considers enhancing the system to include the following reports:

- The items sold. i.e. A breakdown of all the items sold. Such a report is needed for re-ordering and stock control purposes.

- The total number of starters, main courses and desserts sold during a particular session.

As part of the audit, NAO also enquired on the back-ups/restore procedure in connection with this software application. NAO noted that although this software application is hosted and backed up daily on the main server the ITS has never tested these back-ups and does not even have an off-site storage of back-ups. NAO therefore recommends that the ITS periodically performs a test restore of the software application data from back-up so as to ensure that this can be done successfully should a disaster occur. NAO also recommends that an off-site back-up storage facility is available as recommended in Section 4.3 of this report.

Palms Cafeteria

Pembroke Restaurant

Vaults Restaurant

Figure 5: HQ Horizon Food and Drink Edition Screens

3.1.4 Intact Business Management System

NAO noted that ITS paid a yearly license fee to use the Intact Business Management System. Upon enquiring further, NAO was informed by management that this package was procured in order to maintain an electronic version of the inventories.

During the course of this audit, NAO noted that as detailed in Section 2.7 of this report the Inventory officer at ITS keeps all the records on a spreadsheet.

NAO noted that the Intact Business Management System has the potential to offer much more than inventory management and is advertised as a software application that can run an entity's entire business. Such software application is marketed to include a financial package module, credit control, an E-POS functionality, a client-relationship management module and a marketing and business intelligence module. NAO also noted that the yearly licence fee being paid by ITS suggests that ITS may not be licensed to operate all the above mentioned modules. Since NAO, did not manage to find evidence that this software application is installed on any of the Institute's PC's, NAO cannot conclude which modules were given to ITS. Furthermore, upon enquiring with both the IT unit and management, NAO noted that the latter were both unaware of this situation.

NAO suggests that ITS management reviews whether this software application is needed and cease to pay its license fees if it will not be used.

3.1.5 Library - WiSDoM 4

The library system is a tailor made solution built by a local third-party IT company, upon the WiSDoM 4 Enterprise Resource Planning solution.

All the books procured by the ITS Resource centre are inputted in this Library system recording the cost of the book and the invoice details together with the accession number given. The person in charge explained that all the books are given a unique accession number, which will uniquely label each book in the Resource centre and distinguish it from other copies of the same book.

Students and lecturers are automatically entitled to use the ITS Resource centre. They are expected to fill in a form and give their details to the person in charge, who would input the form details on the system. In return, the system will issue a card with a barcode number that serves as the borrowing card for the respective student or lecturer. Students are supplied with a white card that would entitle them to borrow up to four or six books depending on the level of their course. (i.e. Diploma students are entitled to a maximum of six books whilst all other students are entitled to a maximum of four books). Lecturers are supplied with a bar coded yellow card and are entitled to borrow up to a maximum of six books.

The Resource centre is also open to members of the public who can borrow up to a maximum of three books against a deposit of Euro 50. This deposit is also charged to those ITS students who are not entitled to a stipend.

When a book is borrowed the person's library white/yellow card is scanned together with the books barcode number and a record is kept on the system. This same procedure is again carried out whenever a book is returned to the resource centre.

The Library systems also issues a 1st reminder, a 2nd reminder and a final notice for overdue books. If a book is not returned after the final notice, the borrower is charged the cost of the book together with a fine. A notification of these charges are sent to the accounts department where these will either be deducted from the student's stipend or from the deposit paid.

Through the Library system, one can also search for a book using the book title, the publisher or accession number. One can also check whether a particular book is available, to whom it was lent and when it is due to be returned.

NAO observed that the Library system does not have a user manual and users were trained on the job.

NAO noted that this system is used by two officers who however share the same password which is hard coded in the system and cannot be changed without the supplier's intervention. NAO recommends that the supplier is contacted as soon as possible and separate accounts for each user are created.

During the course of this audit, NAO also noted that this application is installed on one particular PC, which is only used for this system and the two users are unable to use this system concurrently. NAO was informed that this application only works with Microsoft Office 2003 and is incompatible with Office 2007 and therefore was only installed on one particular PC which was running Office 2003. NAO suggests that, ITS holds a meeting with the supplier to discuss any incompatibility issues and find a way how this application can be installed on two PC's.

NAO also noted that the books inputted into this system cannot be searched for by subject and thus a student enquiring about which books are available on a particular subject, depends on the officer's experience and knowledge of the books currently available in the resource centre. NAO suggests that the ITS should discuss this limitation with the supplier.

Furthermore, NAO suggests that this application should be enhanced to offer the functionality whereby all the list books found in the Resource centre are exported to a file, which can be then uploaded in the e-learning platform. In doing so, the ITS would promote the use of the books in the Resource centre and students using the e-learning platform would then be able to view the list of books available online.

NAO was informed that there were instances whereby the supplier took one year to implement a barcode reader and several weeks to add the Diploma field in a hardcoded list of student courses. NAO is of the opinion that, since this same supplier is providing the ITS with timely support on another application, the ITS management should hold a meeting with the supplier and try to come up with a solution to sort out any problems this same supplier may have in offering the same kind of service with this application. Furthermore, NAO suggests that the ITS should establish a SLA with this supplier and ensure *mean time between failures*, the *mean time to repair* and the *mean time to recovery* are clearly defined.

Furthermore, NAO observed that this application is hosted and backed up daily on the ITS main server. NAO also noted that a yearly back-up is done on a compact disc (CD) by the officer in charge, but this is kept on site in a locked cabinet. As mentioned in Section 3.1.1, NAO recommends that the ITS performs a periodic test restore of back-ups to ensure that should an incident occur, the data in this application could be restored from back-ups. NAO also recommends that an off-site storage of back-ups is available as per Section 4.3 of this report.

3.1.6 Hardware Stores - WiSDoM 4

The ITS has a specific and very well organised hardware store that is classified in six different categories namely stationery, cleaning materials, fittings and plumbing, paints, hardware and medical supplies.

NAO notes that, in 2009 ITS implemented a Microsoft Access tailor-made stock control system that was built upon the WiSDoM 4 Enterprise Resource Planning solution by a local third party supplier. As part of this implementation, ITS also undertook the job of re-organising the store, assigning rack numbers and barcoding all items.

NAO observed that the hardware stores have also created a manual stock card for each item in stock, that includes the barcode of the item and another manual card for each employee at ITS who may request a stock item.

When the stock is received, a hardware stores officer inputs the invoice in the system by scanning the manual card of each item received. The officer will input the quantity received, the date, supplier, invoice details, the cost of the item, its category, the shelf location and rack number in the system. The quantity of stock items received and their respective costs are also listed on the manual card.

Members of staff who require any items from the hardware stores, are to fill in a uniquely numbered requisition form and have it authorised by their superiors before submitting it to the hardware stores. The Hardware stores would then find the manual card of the employee making the requisition and scan its barcode so as to load the employee details. Following this the officer would then find the manual stock cards of each item requested, scan the barcode and input the quantity requested in the system. The quantities issued are also listed on the manual stock card and the officer in charge ensures that the quantity left in stock that is listed on the manual stock card tally with the quantity left in stock listed on the computer system.

NAO recommends that since the stock control system has proved to be working as desired, the hardware stores should re-engineer their current business process in such a way as to avoid the duplication of work involved in maintaining an electronic and a manual system.

The hardware stores system also has a list of reports which are used for management purposes including reports showing the items issued per department and the total cost of such items on a monthly basis.

During the course of this audit, NAO observed that the hardware store is manned by three officers who have very distinct roles. Although the stock control system can be accessed by two of these officers, it is actually only used by one particular officer. NAO suggests that management holds a discussion with the store-keeper so as to amend the current work practices and train other users in using this application so as to lessen the dependency on a particular officer.

NAO also noted that ITS were not given any user manuals for this system however training was done on the job. NAO suggests that since this system is only used by one person, the Head of Section should ensure that a document is compiled detailing how the application is used so as to ensure continuity.

Furthermore, NAO noted that although this application is accessible through a login and password, these are not set to expire, passwords are not complex (i.e. can be made up of any amount of characters) and can be re-used. NAO suggests that this application's security should be enhanced by implementing a password policy that would forbid the use of weak or short passwords, implement password expiry and prohibit the re-use of passwords.

NAO noted that this system is not hosted on any of the ITS servers and its database resides on the PC on which it is installed. NAO noted that the system is generally backed up daily on to an external hard drive by the officer using this system. NAO recommends that the ITS liaises with the supplier and transfer the application on to the ITS' main server, which is automatically backed up daily. Furthermore, NAO noted that the back-ups stored on the external hard-drive were never tested. NAO thus recommends that a periodic test restore of such back-ups is done to ensure that data can be successfully restored from back-ups should a disaster occur.

3.1.7 Food and Beverage Manager System

The Food and Beverage Manager is a stock control system used by ITS at the food stores.

The Food Stores use this system to input the receipt of food stuffs and beverages. The officer in charge will input the quantity received, the date, price, supplier and invoice details prior passing on the invoice to the accounts department where it is then processed for payment. Furthermore, when stock items are issued a record is inputted detailing the date, the quantity issued and the person making the requisition. Stock requisitions are currently made through a manual form, which the lecturer completes and sends it to the store.

Through this system the Food Stores can also view or print the last four suppliers of each particular item together with their prices and date of last receipt. Furthermore, the system can generate the reports listed below:

- Stock movements.
- Store requisitions.
- Stock receipts valuation.
- Outlets consumption report.
- Outlets consumption summary.
- Outlets overall consumption summary.
- Stores consumption report.
- Stock valuations.
- Stock re-order report.
- Slow moving items report.
- Cost prices variance report.

Besides the above-mentioned reports, the system enables the user to design specific reports. The reports can be displayed on screen, printed to a file, routed to other printers or printed to a comma-separated values file (CSV) file. The CSV file can then be imported from a spreadsheet application like the Microsoft Excel.

NAO noted that as detailed above supplier details and invoice details are currently being inputted twice namely by the stores and the accounts department. Furthermore, NAO observed that requisition notes are currently being done manually. NAO suggests that a business process re-engineering exercise is carried out with the aim of lessening the duplication of work between the departments and enhance the control on issuing of food stocks and re-order levels. The latter may be done by introducing an online requisition facility through which all requisitions can be recorded electronically and vetted by management who would be given access to this system.

During the course of this audit, NAO observed that this stock control is only used by one particular officer. NAO suggests that management should lessen the dependency on this one particular officer and train other users in using this software application.

NAO also noted that ITS were not given any user manuals for this system and training was done on the job. NAO recommends that since this system is currently being used by just one person, a document is compiled detailing how the application works so as to ensure continuity by other officers.

Furthermore, NAO observed that although this application has a login/password regime, logins are currently made up of just the user initials and passwords can be made up of any amount of characters, can be reused and do not expire. NAO suggests that this application's security is enhanced by implementing a password policy that would forbid the use of weak or short passwords, implement password expiry and prohibit the re-use of passwords.

NAO enquired about the back-ups/restore procedure in connection with this application and noted that although this application is hosted on ITS' main server and is thus being backed up daily, ITS has never tested these back-ups and does not have an off-site storage of back-ups. NAO therefore recommends that ITS periodically performs a test restore of this application's data from back-up so as to ensure that this can be done successfully should a disaster occur. NAO also recommends that an off-site facility of back-ups is available as recommended in Section 4.3 of this report.

3.1.8 E-learning

The E-learning platform is an in-house custom built software application developed by the IT lecturer who is currently also maintaining the system. The e-learning platform can be considered as an interactive communication tool between students and ITS lecturers. Through this e-learning platform ITS lecturers can upload class notes, videos, recordings, tests, homework, grades, assessments etc and give students the opportunity of continuing their learning experience beyond the classroom. The lecturers can upload files up to 50MB in size, but can ask the IT lecturer to upload any files which exceed the 50MB limit.

Students wishing to use the e-learning system need to fill in a form and apply for a user account. This form is submitted to the IT lecturer, who will then create the related user account and inform the student accordingly by e-mail. The lecturers using the e-learning platform, will create an enrolment key which is then given to the students who will use it to be able to enrol to the course and access the course material accordingly. Each course has a different enrolment key and this key is only inputted once by the student, when enrolling to a course.

The e-learning platform offers the facility through which students can submit their assignments online. Although the e-learning platform would still allow students to submit a late assignment, the lecturer can keep tabs on the date and time when the assignment was submitted. Late assignments are corrected but given a lesser mark as per ITS policy. The lecturer can also use the e-learning system to upload the assignment marks or course marks of the students. The e-learning system will automatically average out all the grades and provide the student with the final average mark. The lecturers can then print out a report listing all the global marks and submit it to the registry department where it is inputted in SITS. The lecturers also have the facility to check when a particular student last accessed the e-learning platform.

The first version of the e-learning platform was implemented in 2003 and consisted of an online document repository for both students and lecturers. This site was implemented using an early version of Microsoft SharePoint and was in operation for over a year. During this time, the ITS became involved in an EU funded project intended to establish a network of e-business teachers in the Mediterranean region. As a result of the ITS participation in this programme, the ITS deployed the Modular Object-Oriented Dynamic Learning Environment (MOODLE) version 1.9.4, an open source platform which re-defined ITS e-learning experience. NAO was informed that the ITS intended to upgrade to MOODLE version 2 however some components of the e-learning platform did not work and thus this upgrade was postponed.

Following the deployment of the MOODLE platform, the ITS set up a centre for e-learning technologies (CELT) and embarked on a three-year program during which lecturers where trained and the curricula were adapted to the new exigencies of e-learning by apportioning courses between on-line and formal classroom learning. Moreover, the ITS increased awareness amongst its lecturers regarding the issue of copyright when up-loading teaching material and trained them in content creation for e-learning by using applications like Photoshop, Flash and various video editing software. Lecturers were then expected to formulate their own online teaching material.

Furthermore, the ITS implemented a streaming media server and deployed a solution through which lecturers could film demonstrations or whole lectures and upload them on the e-learning platform.

The ITS e-learning platform presently offers 60 on-line courses, most of which are using a blended learning approach but only one course, namely the part-time tourist guide course can be considered as an actual distance learning course. Furthermore, 21 lecturers (out of a complement of 42) and 421 students (out of a complement of circa 600 full-time and 500 part-time) are registered as active users. The on-line courses uploaded on the e-learning platform vary in their full-utilisation of the technology however circa 80% of them only provide downloads of course material. i.e. About 20% of the online courses are currently utilising the full potential that the e-learning platform offers by including video, animation, on-line coursework, on-line testing and presentations.

NAO commends all the above-mentioned efforts, but suggests that senior management develops an e-learning strategy aimed at realising the full potential of this e-learning platform. In this regard, senior management may decide to make the use of the e-learning platform mandatory for all academic staff. Furthermore, senior management may also decide to forbid the printing or photocopying of notes and mandates that all study material is up-loaded on the e-learning platform.

NAO observed that although an extensive training program was provided to lecturers during the three-year post-implementation, recently only a brief in-service course was organised in 2011. Most of the lecturers that were employed after 2007 were not provided any training in the use of the e-learning platform. In-line with the previous paragraph, NAO is of the opinion that an e-learning strategy aimed at increasing the usage of this resource cannot be successful without establishing a program of on-going training to all participants.

NAO recommends that the CELT, within the ITS, formulates a training program for all lecturers. This training program may comprise of three levels as detailed hereunder:

- **Level 1** – Training in simple use of the e-learning platform as a repository of course material and other course resources;

- **Level 2** – Training in the full use of the interactive elements of the platform including training in formulating on-line tests and coursework through which the student can get a self-assessment electronically; and

- **Level 3** – Ongoing training that would serve as a refresher course and would update the participants with any recently added functionality.

Furthermore, NAO recommends that senior management engages in discussion with its CELT and its academic staff, so as to devise ways through which the students would also be enticed to use this platform. The ITS may opt to create user credentials to all students admitted to ITS and instruct them to access the e-learning system and complete any on-line administrative forms such as applying for Wi-Fi access or applying for a library card etc.

NAO noted that the e-learning was currently being maintained by the IT lecturer who created it and there was no one who could maintain the system in his absence. NAO recommends that another officer is trained on maintaining and upgrading this system so as to ensure continuity.

During the course of this audit, NAO observed that the e-learning system is hosted on a Linux Server, which is located in an annex to the classroom of the IT lecturer. Furthermore, NAO noted that the annex is equipped with a Windows server, which was being used for testing purposes with the intent of migrating the e-learning system from a Linux to a Windows based platform. As mentioned in Section 2.6.3, NAO observed that this room was very cluttered, did not have a fire sensor installed and was accessed by a number of people. Moreover, NAO noted that the power sockets in this room were overloaded with a number of extensions, which might create a fire hazard. NAO recommends that the ITS re-locates all the servers in one room. Furthermore, NAO recommends that such room satisfies the criteria detailed in the recommendations listed in Section 2.6.3 of this report.

NAO acknowledges the fact that the e-learning system depends on the Wi-Fi network and therefore a server re-location in the current Wi-Fi setup, may also entail implementing a direct connection between the main Wi-Fi router and the e-learning server.

NAO noted that the hosting server is currently being administered by the IT lecturer. NAO recommends that the hosting server is administered by an IT administrator knowledgeable both on Linux and Windows platforms. The server administrator should be responsible for the overall management of both the above-mentioned servers, in terms of the physical security, integrity, and safety of the data residing on these servers.

NAO also reviewed the account management of this system and noted that this system is accessible through a login and password. NAO also noted that password complexity rules were implemented and passwords expire automatically after one year. NAO suggests that this period is shortened and passwords should expire at the end of each school term. NAO recommends that the e-learning system would offer the facility through which users can change or renew their passwords online before these expire. In the event that a password has expired or a user has forgotten his/her password, NAO suggests that e-learning system would offer the facility to change password, whereby a new password is generated and sent to his/her e-mail account. When retrieving the new password, the latter must be changed upon first logon. NAO noted that the change or renewal of passwords is currently being handled manually by the lecturer in charge of the system.

NAO observed that the officer maintaining this system, periodically contacts the ITS registry to obtain a list of students who have finished their studies at ITS and terminate their access manually. NAO suggests that the e-learning system would be upgraded in

such a way that students are granted access for the duration of the course and their user account is automatically terminated when the course is over.

During the course of this audit NAO enquired whether the e-learning system adheres to a back-up and restore procedure. NAO noted that although a back-up schedule was established, whereby a partial back-up is taken on Monday and Friday and a full back-up is taken on Wednesday, this was not always adhered to, since back-ups were not scheduled automatically. Furthermore, no back-up logs are being kept to record whether a back-up has failed or completed successfully. NAO suggests that back-ups are done with a daily/weekly/monthly schedule as detailed in Section 4.3. Back-up logs should also be kept and seen to regularly.

Furthermore, NAO noted that, the ITS has never tested these back-ups and does not have an off-site storage of back-ups. NAO therefore recommends that the ITS periodically performs a test restore of the application data from back-up so as to ensure that this can be done successfully should a disaster occur. NAO also recommends that an off-site facility for back-ups is available as recommended in Section 4.3 of this report.

NAO also noted that the ITS had engaged a third-party supplier to back-up the e-learning environment. NAO recommends that senior management reviews the need for this service in view of the fact that back-ups of both the e-learning platform and the data within may be taken by ITS.

NAO also noted that the Linux server is connected to two home UPS, thus giving a total uptime of 30minutes in the event of a power failure. However, NAO recommends that the ITS replaces the current home UPSs with a new UPS that incorporates a network management card. The aim of the network management card is to provide a secure monitoring and control of the UPS via a web browser. The network management card will then be configured to send an e-mail notification to the server administrator in the event of a power disruption. The Linux server connected to this UPS will be installed with a UPS software, which will trigger an unattended shutdown when a power failure is detected. Furthermore, if the Linux server has two power supplies, these can be connected to two different UPSs. In the event of a hardware malfunction on one of the UPS, the server will remain switched on as the load will be shifted on the remaining UPS.

3.1.9 OPERA Property Management System

OPERA Property Management System (PMS) is an off-the-shelf package that runs on an Oracle Database and is used by hotels for managing front desk, housekeeping and accounting activities. Since this package is used by a large number of hotels, ITS included a specific course module so as to teach this package as part of the front office theory to help students gain the required skills. The version of OPERA PMS being used by ITS is Version 4.

OPERA PMS was designed to meet the varied requirements of any size of hotel or hotel chain and provides all the tools hotel staff need to perform the following daily operations: handling reservations, checking guests in and out, assigning rooms and managing room inventory, accommodating the needs of in-house guests and handling accounting and billing. This software application operates in either single-property or multi-property mode, with all the properties in an enterprise sharing a single database. The key features of this software application are:

- **Reservations** — The software application provides a complete set of features for creating and updating individual, group and business block reservations, including deposit handling, cancellations, confirmations, waiting lists, room reservation blocking and room sharing. The Reservations features are integrated with other functionality such as profiles (defined below), cashiering and deposits.

- **Rate Management** — Opera PMS includes a set of features for setting and automatically controlling rates for services, generate rate quotations, forecast revenue and generate rate analysis.

- **Profiles** — Opera uses profiles to store details about the guests, companies, agents, business sources, contacts and groups that the hotel does business with. A profile would include names, addresses, phone numbers, e-mail address, membership enrolments, stay and revenue details, guest preferences as well as reservation and stay histories and other statistical data. Since this software application is only used for training purposes ITS have populated it with sufficient dummy data. Having this profile information in hand makes it easy for students to practice at creating reservations for guests, processing commissions for agents, preparing billing statements, constructing mailings, managing membership programs, collecting accurate statistics and performing many other Opera related tasks.

- **Front Desk** — handles individual guests or groups, and has features for room reservation blocking, managing guest messages, wake-up calls, creating and following up on inter-departmental advisories.

- **Back Office Interface** — revenue transfers, market statistics transfers, daily statistics transfers and city ledger transfers can be made from OPERA PMS to a back office system.

- **Rooms Management** — handles all facets of room supervision including availability, housekeeping, maintenance and facility management. The Queue Rooms feature of the property management software coordinates Front Office and Housekeeping efforts when guests are waiting for rooms which are not immediately available for assignment.

- **Cashiering** — posting guest and passer-by charges (including taxes and other generates), making posting adjustments, managing advance deposits, settlements, checkout and folio printing. Cashiering accommodates multiple payment methods per reservation including cash, cheques, credit cards and direct bill. In multi-property environments, guest charges can be cross-posted from any property in the hotel complex.

- **Accounts Receivable** — includes direct billing, invoicing, account aging, bill payments, account research, reminder and statement generation.

- **Commissions** — calculates, processes and follows up on travel agent and other types of commission payments.

- **Reporting** — OPERA PMS includes a large number of standard reports but can also be customised for each hotel and new reports may be created as needed.

- **Fully Configurable** — OPERA PMS is fully configurable in terms of system behaviours and priorities, and system-wide defaults which are controlled by the property. User permissions determine which property management software features may be accessed by each user and user group. Many OPERA screens may be customised by property.

- **Global Perspective** — supports multi-currency and multi-language features to meet the requirements of global operations. Rates and revenues can be dynamically converted from the local currency to any other currency. The appropriate language for guest correspondence can be automatically determined by the guest's profile language; country-specific address formats are supported.

- **Hospitality System Interfaces** — OPERA PMS includes interfaces to hundreds of third-party hospitality systems including yield management, telephone and electronic switching, TV and video entertainment, key lock, restaurant POS, activities scheduling, minibar, and wake-up call systems.

Furthermore, OPERA PMS also has a floor plan depicting which rooms are occupied and uses colour coding to show at a glance the housekeeping status of each guest room. The user could also view room and room type information. This option could also depict a layout of each floor including guest rooms, interconnecting rooms and other physical features such as stairways, vending areas, exits, and elevators.

The OPERA PMS has a login and a password which is made up of a unique string of characters having a minimum length of six characters; the maximum length is ten characters. NAO noted that since this system is being used for training purposes only, the lecturer, who also has administration rights on this system, has created eight accounts (one per pc) which the students use during their practical sessions.

OPERA PMS also has an online Help facility which will automatically show the help page for the current window i.e. If Profiles window is displayed on screen the F1 key will display help page for Profiles. The OPERA PMS also has a lot of Quick Keys. Using these keyboard shortcuts a user can load different screens instantly.

NAO noted that this system is hosted on ITS main server and is thus being backed up daily. Furthermore, NAO observed that the related lecturer maintains two replicas of this system's data, one used as a production system that contains all the rates and profiles and the other used as a class training system. Should something happen to the class training system the lecturer can copy the production system and resume lectures normally.

During the course of this audit NAO noted that this software application is installed in a particular lab (Room 101). NAO noted that the PC's in this lab need to be replaced or upgraded as lately these were giving a lot of problems. NAO also noted that currently the system is being administered and maintained by the lecturer. Given that the lecturer is not a trained system administrator, the local supplier is being requested to provide the additional support required as a result of the above situation. NAO

recommends that the IT unit takes over the administration of this system and at least carries out everyday tasks like setting up printing rights or installing and setting up the system after PC formatting.

NAO also noted that the Version of OPERA PMS used by ITS is Version 4 and upgrading this system to version 5 would enable the lecturer to teach the new features available in this version and currently being used in the industry. NAO was informed that senior management is discussing upgrading this system.

3.2 Web

3.2.1 Website

The ITS has a website with the following Uniform Resource Locator (URL) www.its.edu.mt which is hosted and backed up by a third party supplier. During the course of this IT Audit, NAO reviewed the ITS website and noted that this is an intuitive website which is updated regularly.

This website provides current and prospective students with the information they may require including information about ITS, any forthcoming events, vacancies in their related industry and news. Furthermore, this website is also providing valuable information to members of the general public who may be interested in this sector, the Institute's restaurants or resource centre.

Whilst reviewing this website NAO noted that:

- The Links page includes three broken links to the *City and Guilds, Employment and Training Corporation* and *Malta Tourism Authority* websites that need to be updated.

- The Library catalogue search screen has a drop down box for the *"subject term"* which includes test data entries (TEST2, Test3, test4) that need to be removed.

- That the website is not compliant with the Government's *"Website Content and Presentation Standard"* GMICT S 0051-1:2011 and does not include:

    - A copyright notice;
    - A privacy policy (refer to Annex E for guidance);
    - An accessibility statement. (refer to Annex F for a template);
    - A help facility. NAO notes that the Institute's website is albeit a very intuitive website and the Help facility need not be an extensive one.
    - The gov.mt logo that links to the Government portal (http://www.gov.mt); and
    - A printer friendly version of pages that are likely to be printed.

3.2.2 Facebook

NAO notes that nowadays various entities worldwide regularly rely on social media to engage with their customers. Social Media has integrated technology, social interaction and content creation to collaboratively connect online information. Through social media, people or groups can create, organise, edit, comment on, combine, and share content.

NAO recognises that social media may help entities in achieving their mission and if leveraged to its fullest, may create the opportunity for greater collaboration between entities and departments, help management in decision making, engender more experimentation and be a tool through which an entity gets timely responses from the public.

ITS has recognised the potential of social media as a modern communication channel and in May 2011 set up a Facebook page to market the Institute. This page has over 700 likes and is most popular with the 18-24 year old age group. This page also includes photos taken during various events and a number of videos including demonstrations of various cocktail preparations and others featuring final year projects.

During the course of this audit NAO reviewed the ITS' Facebook page and noted it was last updated in February 2013. Furthermore, NAO noted that the videos section includes videos featuring 2010 final year projects but did not feature the student projects of 2011 or 2012. NAO noted that ITS' Facebook page was created and is still being updated by top management. Given that content management is a fairly time consuming activity, NAO suggests that this function is delegated to an officer.

Furthermore, NAO noted that the *"Welcome to ITS"* page was created with a commercial management platform, which was only licensed for a trial period and has now expired resulting in an empty page. NAO recommends that ITS recreates this page.

Moreover, NAO noted that the *"Contact Information"* page is listing the names of employees who are no longer working at ITS. NAO therefore suggests that ITS either updates the names accordingly or removes the names and refers only to the titles of such persons to identify them.

Chapter 4

Information Technology Operations

Chapter 4 - Information Technology Operations

4.1 Anti-virus software

NAO recommends that the ITS considers purchasing an anti-virus solution, that can be centrally managed from one administrator. Such a solution will allow the administrator to:

- create configuration files for the various types of computers being managed;
- create push install packages through which the IT administrator can automatically deploy the anti-virus over the network without sitting in front of the destination machine or depending on the user to do this;
- provide updates across the LAN. The IT administrator would pull down the update once to the main server, instead of having all pc's pull down the updates from the internet (reducing network traffic);
- monitor clients;
- set-up anti-virus policies to block known and unknown threats, such as password cracking software applications, block anti-virus software from being disabled or uninstalled etc.;
- issue periodic reports detailing which computers were infected with malware, if the malware was removed, if all the PCs and Laptops are updated with the latest update etc.

Apart from having a sound anti-virus solution that is adequate for the entity's needs, NAO also believes in educating the users. Generally, viruses and worms get into a network through unsolicited e-mail messages, also known as spam. Educating users on how to deal with spam effectively can help reduce the chance of viruses and worms. NAO thus suggests that the ITS, informs its users on the dangers of e-mail attachments and viruses. This may be done through periodic e-mail shots or posters on notice boards etc.

4.2 Patch Management

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

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

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

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

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

To mitigate risks related to malware and security exploits, NAO observed that the ITS adopts two different approaches when applying patch management on servers and workstations. While all workstations have been configured to automatically download and install product updates through the Microsoft Windows update tool, the IT unit deploys product updates manually on the servers maintained by them and depends on the supplier and the IT lecturer to deploy product updates on the other servers.

NAO recommends that as best practice, a hotfix or a service pack is initially deployed on a testing server and then deployed on the other servers if no abnormal behaviour was observed. The IT Unit should ensure that the server is backed up successfully, prior to installing any security or critical update.

4.3 Back-ups and Off-site Storage

NAO observed that ITS has a NAS device installed in the main server room. NAO noted that one of the servers is being mirrored onto this NAS device whilst another two servers are being backed up onto a cloud managed by third-party suppliers. NAO recommends that all servers are backed up onto the NAS system and that a tape drive is used to back-up the NAS device in a reliable and secure back-up method such as the Grandfather-father-son back-up methodology. This *"Grandfather"* method uses a rotational system of three sets of back-ups as detailed below:

- the daily back-up – done on the "son tapes";
- the weekly back-up – done on the "father tapes";
- the monthly back-up – done on the "grandfather tapes".

ITS may also opt to mirror the NAS system onto a replica NAS system instead of backing it up on tape. Although back-up tapes are considered a reliable source as long as they are properly stored in a secure safe (free from any environmental issues), the use of the tape drive, tapes and storage can be costly. ITS should thus evaluate these two options accordingly. Should ITS decide to mirror the NAS system on a replica NAS, the latter can then be placed in a different room/office so as to achieve a degree of off-site storage.

NAO also observed that, no back-up logs are being kept to record whether a back-up has failed or completed successfully. NAO suggests that these are kept and seen to regularly.

Furthermore, NAO suggests that, considering that the ITS has three virtualised server environments, the ITS should consider investing in a back-up solution that is also capable to back-up the virtual server environments.

The ITS should also set-up an off-site storage facility where the weekly and monthly tapes can be stored. This off-site storage area may consist of a safe stored away from the server room either in the main premises or at the MLK premises.

Furthermore, NAO suggests that should ITS implement the recommendation detailed in Section 2.6.1, whereby a dedicated server is setup at MLK, the above recommendations in terms of back-ups and off-site storage should be implemented vis-à-vis this server too.

4.4 Electronic mail and Internet Services

NAO considers e-mail and Internet Services as mission critical services and principal vehicles for electronic communications both within the ITS and with external entities.

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

NAO suggests that the ITS should periodically remind its employees about the salient points highlighted in the e-mail and Internet services directive especially the restrictions on use of e-mail and Internet services as reproduced in **Annex D**.

During the course of the audit, NAO observed that certain members of staff do not have an e-mail/internet account and were using the e-mail accounts of their superiors when they need to correspond with external entities and suppliers. NAO, recommends that the ITS management reconsiders this malpractice and ensure that e-mail is provided to all the members of staff who require e-mail access.

4.5 Wi-Fi facilities

As detailed in Section 2.6, the ITS has a 30 Megabit Internet and Wi-Fi connection, which is being maintained by a third-party supplier.

NAO observed that at the initial stages of this IT audit, the wireless network was an unsecured network intended for student use. However, due to the fact that this wireless network was unsecured and accessible to everyone within the ITS premises, the students, members of staff and the general public who happen to be in the area, were in a position to gain access to this wireless network connection. Based upon NAO's recommendation, the ITS' management instructed the supplier to implement an authentication system whereby students and academic staff are provided with an account to gain access to the wireless network. NAO commends the immediate action taken by the ITS management in this regard. However, during subsequent visits NAO noted that the authentication system implemented was not working in some parts of the building, and login accounts were granted to certain administrative staff who also happened to have access to the Government Network. During the course of this audit, NAO noted that the IT unit had changed all the student passwords and provided the students with identical passwords.

Although the immediate action taken by management to secure this network, is deemed by NAO to be a step in the right direction, the ITS must ensure that:

- Wi-Fi security is monitored and ensured at all times and in all parts of the building;

- A clear segregation is done in such a way that people/devices accessing the government network would have no access to the Wi-Fi network. NAO suggests that since the Wi-Fi facilities were procured for student use, the administrative staff should not have access to such facilities. Such measure would also indirectly address issues of productivity by preventing staff from accessing online games, social networking sites etc.

- It complies with the Government's Policy and directive vis-à-vis Wireless technology. (GMICT Policy P 0047:2007 Wireless).

During the course of this audit, NAO also conducted site visits in all labs both at the ITS (St. Julian's) and the MLK premises. NAO noted that the PC's in Room 103 and Room 102 are connected to both the Wi-Fi network and the Government network. NAO suggests that this is reviewed to verify whether this may constitute a vulnerability to the government network. NAO notes that a meeting between the ITS senior management and MITA's Chief Executive Officer (CEO) was held in this regard.

4.6 Web filtering

During the course of this audit, NAO found indicative evidence suggesting that the Wi-Fi connection could have been used to play online games, to download films, music etc. This was highlighted to senior management who took immediate action and instructed the supplier to implement a filter through which access to pornographic material and Peer-to-Peer (P2P) is blocked.

Senior Management explained that the original purpose of this connection was two-fold; firstly as a learning tool for students and secondly for entertainment purposes by students during their free lessons. Consequently, NAO understands that filtering this connection further may not be a solution. NAO would therefore recommend that students are from time to time reminded that this connection is to be used responsibly especially vis-à-vis bandwidth hungry sites like video-on-demand sites or heavy downloading. Furthermore, the IT unit may monitor this connection from time to time and provide senior management with a list of heavy bandwidth users. Senior Management may then decide whether this use was justified and approach the users accordingly.

NAO recommends that ITS explores solutions whereby websites are filtered by category, thus allowing gaming and video-on-demand only in certain areas of the building. Using the mentioned solution different filters can be applied for different computers, based on Internet Protocol (IP) addresses/location on the network. Therefore a student residing in the canteen doesn't get the same filtered content a lab student does. The filtering software would possibly have the option to set custom filters to white list and black list specific sites. By doing so ITS would strike a balance between allowing students to use the internet for recreational purposes and at the same time stop internet misuse in class or in places like the resource centre. This filter should also prevent P2P software, therefore preventing a substantial increase in bandwidth consumption. Reporting must also be available in the solution used, in order for ITS IT Unit to clearly understand internet usage in the entity.

Furthermore, NAO observed that administrative staff were using the Wi-Fi connection instead of the Government network for internet browsing. Consequently, NAO interviewed various members of staff and noted that the web filtering on the Government network may not be adequate for the ITS. Various members of staff stated that the Government network prevented them accessing certain sites which they need in fulfilling their duties such as sites about wines that are deemed by the web filter on the Government network as Alcoholism. NAO thus suggests that the IT unit gathers a list of such sites/categories and holds a discussion with MITA so as MITA could allow access to the “Health package” as per MITA_SCC-FAQ-Internet-FilteringPackages-v1.1 document as per the Institute’s needs.

4.7 Multi-Function Printers

NAO noted that ITS purchased multi-function printers one of which is also installed at the MLK building.

NAO notes that these machines are made up of a combination of printer, scanner, photocopier and have the capability of printing double sided, scan documents and e-mail them automatically etc.

NAO however observed that these multi-function printers are mainly being used as photocopiers and some of which, like the one at MLK, are not even connected to the internal network (Refer to Section 2.6.1).

NAO also observed that most of the printing is done using stand-alone printers which are installed in all the offices. NAO recommends that ITS phases out stand-alone printers and consolidates the printing to these multi-function printers. By doing so, ITS senior management will cut the maintenance costs in servicing, supporting and purchasing consumables for such a large number of stand-alone printers. Furthermore,

ITS senior management would be able to control and manage printing as it would know what is being printed and which users are engaging in heavy printing. Such a move will also reduce energy consumption and in the long run reduce purchasing costs of stand-alone printing and scanning equipment.

NAO recommends that ITS configures these multi-function printers in order to have features such as scan to e-mail and secure printing, where applicable, in order to fully utilise this equipment. NAO also recommends that ITS configures these machines as network printers, considering that they are more robust. By having these printers connected to the network, ITS could install software to audit and log printing on the mentioned printers. Such software would offer real-time activity logs, and therefore will surely be useful for ITS IT Unit to ensure that there is no misuse of the equipment.

NAO also suggests that users at the main building should be given access to at least two multi-function printers so that if one is unavailable, the user would have the option to use the other one.

Furthermore, NAO suggests that ITS assigns a predefined range of IP addresses for printers/network devices and configures the dynamic host configuration protocol (DHCP) reservations for all network printers and other network devices, in order to follow best practice and prevent running into IP conflicts, therefore avoiding unnecessary waste of time on ITS IT Unit searching the physical location for any conflicting IP addresses.

4.8 Physical Security

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

4.8.1 Stored Documents

NAO noted that the ITS do not have an archive where documents are stored. Instead documents are kept in various metal filing cabinets in all offices around the building.

NAO recommends that as a best practice, employees should be asked to:

- keep filing cabinets locked at all times;
- label all documents and files in such a way that these can easily be found; and
- shred any unwanted or extra documents which are no longer needed.

4.8.2 Server Room

An organisation's server room is the heart of an entity's physical network, and someone with physical access to the servers, switches, routers, cables and other devices in that room can do enormous damage.

As detailed in Section 2.6, the ITS has two server rooms, one of which is an annex to a classroom and the other one is a server room equipped with a fire sensor, NAO recommends that all servers are migrated to the original server room and that this room:

- is fitted with an air-conditioning system which is kept on at all times;
- is kept under lock and key and a log is kept of who accessed the room with the date and time;
- has no curtains, fitted carpets and other fire hazardous décor;
- is equipped with an adequate fire extinguisher that is serviced regularly;
- is equipped with a fire alarm system;
- is kept clean and free from clutter;
- is to be secure i.e. windows should lock securely and iron bars should be installed if windows are easily accessible;
- all cabling in this room is labelled and passed through proper trunking. The cabling should also be organised in an orderly fashion that is manageable and that fits well in the network cabinet;
- is equipped with a humidity/temperature monitor that sends alerts via email/ sms if it reaches a pre-defined threshold.

NAO recommends that until migration of servers from the classroom's annex room to the server room is done, the ITS should clean the annex room and free it from all clutter.

4.8.3 Buildings

NAO noted that the ITS has implemented a number of physical security measures throughout its buildings namely:

- a Closed-Circuit Television (CCTV) system which monitors entry and exit to the building and ITS' offices;
- 24 x 7 security personnel;
- a visitor's policy is in place (at the main building) whereby the security personnel log visitor details and provides them with a tag;
- smoke detectors are installed throughout the building. These are inspected and tested regularly by the supplier;
- fire extinguishers (Carbon dioxide and Water) and fire hoses are available at various points throughout the building. Fire extinguishers are also inspected on a regular basis by a local supplier;

- a back-up generator is available; and
- the server room is kept locked at all times and accessed by a limited number of staff.

Whilst commending all the above measures NAO noted that the visitor's policy is not applied at all times and visitors are sometimes allowed access to the building without registering. NAO therefore suggests that the security personnel are made aware of the importance of the visitors register and ensure that all visitor entries are logged.

Furthermore, NAO recommends that:

- A visitor's policy like the one in place in St. Julian's, is applied at the MLK building whereby the particulars of all visitors are noted on a register and visitors are given a tag.
- The ITS considers installing metal bars in all ground floor windows at the MLK building since all windows are reachable from road level.
- The ITS considers installing metal bars in the windows of Room 103 at the Main building where a considerable investment has been made.
- The NAO recommends that ITS ensures that power sockets including the ones in the labs are not overloaded with extensions.

4.8.4 Closed-Circuit Television (CCTV)

The ITS main building in St. Julian's is monitored by a set of 32 infra-red surveillance CCTV cameras, that record any movements on a hard disk. Recordings of approximately one month are generally available and are accessible to senior management only. NAO suggests that the CCTV in the resource centre is re-configured so as to cover all angles of the room and lessen the incidents of theft.

The MLK Building is also monitored by a CCTV system made up of ten infra-red surveillance cameras, that record on a hard disk. Recordings of approximately two weeks are generally available and are accessible to senior management only. NAO noted that surveillance cameras at MLK do not however cover all the strategic areas of this building. NAO therefore recommends that management liaises with the security officer at MLK to investigate how this could be improved.

Chapter 5

Information Security

Chapter 5 - Information Security

NAO has observed that the ITS has no formal documented risk assessments and no business continuity and disaster recovery plans.

NAO has however noted that although the ITS has no formal documented plans, the head of administration has discussed business continuity with both the IT Unit and management. Furthermore, NAO notes that the ITS implemented a system through which the main server is currently being mirrored on a NAS device.

NAO thus suggests that a business impact analysis and a risk assessment exercise are carried out from which a business continuity plan that includes a disaster recovery plan is drafted.

5.1 Business Impact Analysis

Business impact analysis is an analytic process that aims to reveal business and operational impacts stemming from incidents or events. A business impact analysis should lead to a report detailing likely incidents and their related business impact in terms of time, resources and money. This report should basically give an understanding of the impact of non-availability of the systems on the business (in various dimensions such as loss of revenue, loss of profits, inability to comply with statutory norms, damage to reputation and image, etc.).

The business impact analysis is to be based upon information that is collected from academic staff, heads of Departments and other key persons within the ITS. The information could be collected using different approaches. One of the popular approaches is the questionnaire approach whereby a detailed questionnaire could be circulated to key users in IT and to the end-users. Another alternative is to interview groups of key users. The information gathered during these interviews or from the questionnaire response is to be tabulated and analysed so as to develop a detailed business impact analysis plan and strategy.

NAO recommends that the ITS lists and reviews its critical and non critical functions. For each critical function the ITS should then determine the:

- **Recovery Point Objective** - the acceptable latency of data that will be recovered ensuring that the Maximum Tolerable Data Loss is not exceeded; and

- **Recovery Time Objective** - the acceptable amount of time to restore the function ensure that the Maximum Tolerable Period of Disruption for each activity is not exceeded.

After going through this process the ITS should then determine its recovery requirements, which will consist of the following information:

- The business requirements for recovery of the critical function; and/or
- The technical requirements for recovery of the critical function.

5.2 Risk Assessment Exercise

NAO is of the opinion that a cost-effective business continuity and disaster recovery plan need to be part of a disciplined risk management approach, which should include an analysis of business processes and the risks that these processes are exposed to. An entity, that fails to identify its risks or processes, can neither manage the risks nor realistically plan for their consequences. A realistic risk assessment is therefore vital for the cost-effective management of the ITS' risks.

NAO recommends that the ITS identifies and documents its risks, taking into account all types of threats that can impact the ITS' business. Fires, floods, hurricanes, acts of terrorism/sabotage, hardware/software failures, virus attacks, denial of service (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.

The ITS should then document the probability assessments and devise alternative solutions that may be deployed to mitigate the risk to the business and the potential costs associated with each solution.

5.3 Business Continuity and Disaster Recovery Plans

The ITS should also have a formal and documented business continuity and disaster recovery plan designed to reduce the impact that disruptions might inflict on the entity's operations.

The Business Continuity Plan should:

- include a list of essential hardware, software and information;
- identify an alternate site from which to resume operations;
- preferably include details of manual processes that could temporarily maintain operational functionality for each business process in the event of a total IT system collapse;

- include a Disaster Recovery Plan that amongst others lists the access rights granted following a restore;
- include a plan that details how to restore operations to normality;
- 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 amongst the key persons, support staff and employees to be adopted during recovery of services;
- be documented and written in simple language and understandable to all;
- be periodically tested and updated so as to ensure it is kept current;
- be stored in hard-copy and soft-copy format both on-site and off-site; and
- be distributed to members of staff, Head of Sections etc. (any confidential information should only be given to key persons on a need to know basis)

Furthermore, the Disaster Recovery Plan should stipulate the procedures that are to be taken into account in the event that the IT facilities become inoperative due to extreme incidents. It should also document the recovery approach, the recovery time objectives and the sequence of events including the pre-requisites, the dependencies and the responsibilities assigned to every individual involved in the plan.

Apart from having a Disaster Recovery Plan, the ITS should ensure that the SLAs it has with its suppliers cater for adequate and timely maintenance, support and business continuity.

5.4 Security Awareness Training

NAO acknowledges that the best way for an entity 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.

Such training may be done as part of the induction session given to new employees and should also be part of an ongoing programme through which employees are kept updated with the entity's new policies. NAO recommends that security awareness should be part 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. 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.

NAO recommends that the ITS issues a set of computer security awareness guidelines both for staff and students. The aim of such guidelines should be to:

- teach users how to protect their computers and their personal information;
- inform the users about the security risks of the Internet and highlight the appropriate actions that could be taken to reduce those risks;
- explain how the Institute's network is set up whereby all the websites are being filtered and those deemed as unsuitable or undesirable are blocked;
- give 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;
- explain the importance of passwords, account management, etc. and discourage sharing of logins and passwords.

Chapter 6

Management Comments

Chapter 6 - Management Comments

The following comments were submitted by the ITS by way of management comments.

The management of the ITS welcomes the recommendations put forward by the NAO, which findings are presented in the report.

- The securing of Wi-Fi has been monitored and the situation is now solved. In addition, the management organised a preliminary meeting with MITA to further tackle the issue of IT security amongst other matters such as the development of a contract between the two organisations.

- The purchasing of IT equipment is carried our according to public procurement regulations.

- The ITS fully acknowledges the need for a qualified Head of IT who can facilitate and implement most of the recommendations present in this report.

- The recruitment of a qualified head of IT also means that a holistic ICT strategy and policy can be developed. The management acknowledges the recommendations put forward by the NAO in this regard.

- In due course the ITS will be engaging in a cost/benefit analysis to come up with a feasible ICT process.

- Logging of IT related maintenance has been put in place, under the supervision of the Head of Administration (in the absence of a Head of IT)

- The management will be contacting third parties to introduce a data protection clause in the agreements.

- Supplier of SITS has been contacted and the management is exploring the possibility of an upgrade as well as a revision of the current maintenance agreement.

- An e-learning strategy will be devised in collaboration with the person responsible for the platform, as well as with the newly recruited Head of IT.

- Management is planning a revamp to the current website and the recommendations put forward by the NAO will be taken into consideration. Furthermore, the Facebook page is being updated, and the contact information updated accordingly.

Finally the management would like to thank the NAO auditors and their respective directors for their support throughout the audit process.

Annexes

ANNEX A: ORGANISATION CHART

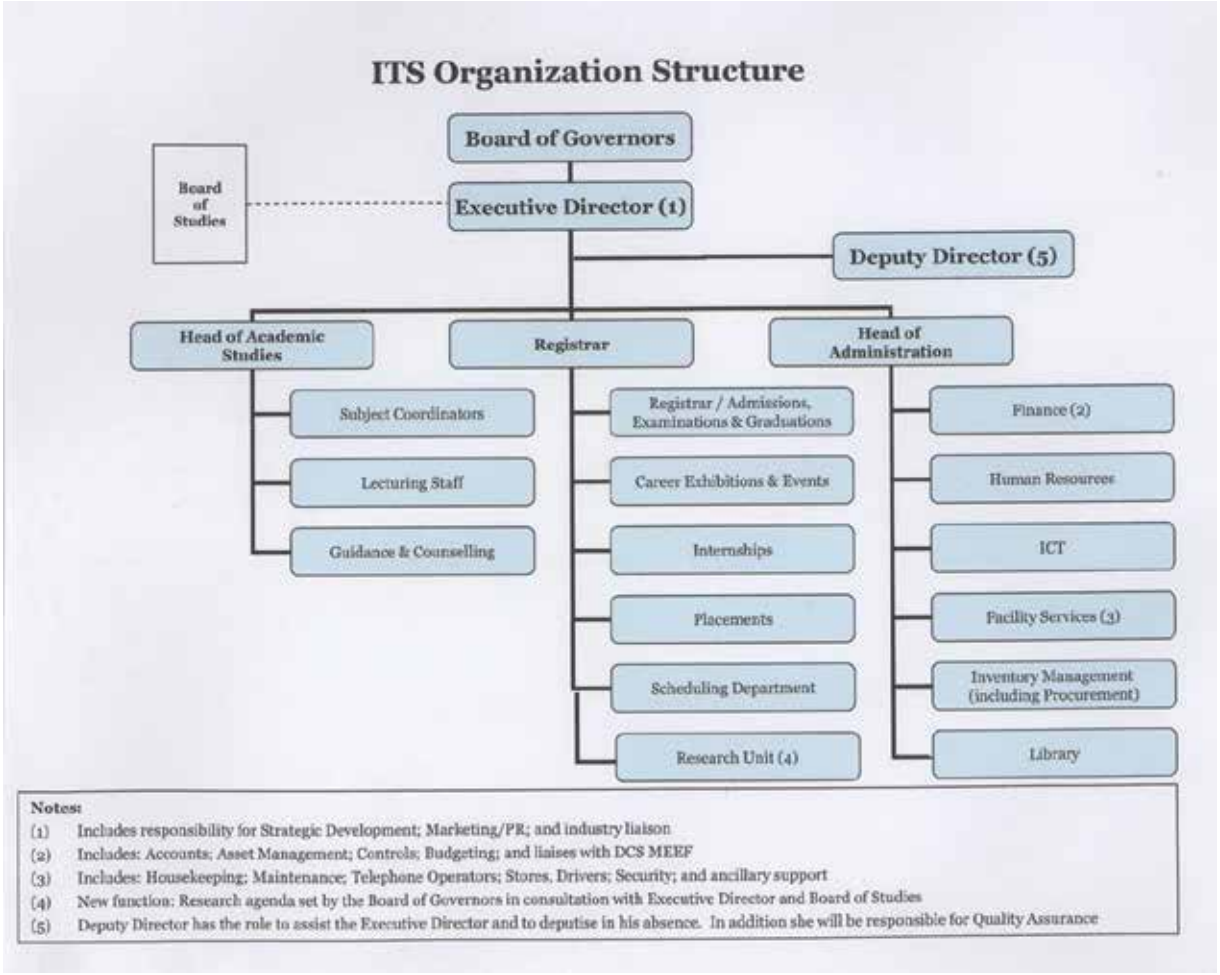


Figure 6: Organogram of the ITS

ANNEX B: COBIT CONTROLS

CoBit defines IT activities in a generic process model within four domains[2]. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate as depicted in Figure 7. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

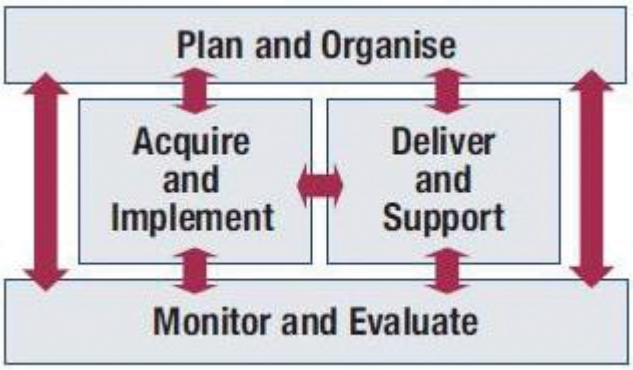


Figure 7: The four integrated domains of CoBit

Plan and Organise

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

Define a Strategic IT Plan

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

Assess and Manage IT Risks

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.

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

Acquire and Implement

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

Manage Changes

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

Install and Accredit Solutions and Changes

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

Deliver and Support

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

Define and Manage Service Levels

Effective communication between IT management and business customers regarding services required is enabled by a documented definition of, and agreement on, IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. 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 minimises the business risk associated with non-performing suppliers.

Ensure Continuous Service

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

Ensure Systems Security

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

Manage the Physical Environment

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

Manage Operations

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

Monitor and Evaluate

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

Provide IT Governance

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

ANNEX C: SOFTWARE PROJECT LIFE CYCLE

NAO suggests that a typical Software Project Lifecycle should seek to address the below questions:

Feasibility/Requirements Study Phase

- What is the main objective to be achieved with the implementation of the software application?
- What is the cost/benefit analysis of the project?
- What data is required to meet the application's goals?
- What are the business processes that the software application would have to cater for?
- Will the software application be required to integrate with any existing systems and infrastructure?
- Who are the intended users?
  - What is their level of IT Literacy?
  - What is their level of expertise with the subject area?
  - Under what circumstances will they use the software application?

Design Phase

- How will the required input data be obtained (ex. from a database, form or through drop-down lists)?
- How will the input data processed to achieve the desired output from the system? During this phase the business process must be incorporated into the design.
- What form will the output take (ex. a report, exported to a file, saved as an image)?

Development Phase

This stage would generally involve managing the supplier or developer chosen. Furthermore, during this phase, one would need to answer the questions below:

- What additional hardware/software would this software application require?
- What are the hosting requirements of this software application?
- How will this software application be implemented?

Testing Phase

- Does the application function as expected?
- Does the application meet the requirements set forth in the requirements study phase?
- Does the application meet the user acceptance testing criteria?

Implementation Phase

This phase would generally involve the implementation of the system, user training and support. One would need to determine the following:

- Is there a plan for the implementation of the system?
- Who will train the users? Have the related resources been booked?
- Who will be providing the necessary support?
- Has an SLA been signed?

Maintenance Phase

- What are the issues identified post-implementation?
- How can the above issues be resolved?
- Are there any foreseen enhancements to the system? *

* Enhancements are to be considered as extensions to the software and thus one should follow the lifecycle from the beginning.

ANNEX D: RESTRICTIONS ON THE USE OF ELECTRONIC MAIL AND INTERNET SERVICES[3]

Restrictions on the use of e-mail services

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

- Impersonate or forge the signature of any other person when using e-mail;
- Amend messages received in a fraudulent manner;
- Gain access to, examine, copy or delete another person's e-mail without the necessary authorisation from the person concerned;
- Disclose their password or other means of access;
- Use someone else's password or other means of access to a computer;
- Use e-mail to harass or defame any person or group of persons;
- Use e-mail to conduct any personal business or for commercial or promotional purposes;
- Send as messages or attachments items that may be considered offensive, pornography, illegal material, chain letters or junk mail;
- Send e-mail in bulk unless it is formally solicited;
- Place Government-assigned e-mail address on non-official business cards;
- Send trivial messages or copy messages to people who do not need to see them;
- Send unsolicited mass e-mailing to more than twenty-five e-mail users, if such unsolicited e-mailing provokes complaints from the recipients; and
- 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.

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

Restrictions on the use of Internet services

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

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

ANNEX E: PRIVACY POLICY

The below is an extract from the Government's "Website Content and Presentation Standard" GMICT S 0051-1:2011 which may be used as guidance.

Privacy Policy

The Website shall include a Privacy Policy statement stating:

- that any personal information collected shall be stored or processed in accordance with the Data Protection Act;
- that any personal information submitted by Website users in a query will only be used to respond to that particular query;
- whether any non-personal information will be collected and if so, which information and the purpose of its usage;
- the information on any cookies used, including why they are being used and what information is being recorded or relayed; and
- the rights of the data subjects as per the Data Protection Act.

ANNEX F: ACCESSIBILITY STATEMENT

The below is an extract from the Government's "Website Content and Presentation Standard" GMICT S 0051-1:2011 which may be used as guidance.

Accessibility Statement

The Website shall carry an accessibility statement which declares that the website caters for individuals with disabilities.

Statement shall read as follows:
Every effort has been made to ensure that this website is accessible to persons with disability. If you have any difficulty accessing information on this website please contact us and we will do our best to assist you.

Recent NAO Publications

NAO Audit Reports

April 2011	Performance Audit: Achieving a Healthier Nutrition Environment in Schools
May 2011	Enemalta Corporation Tender for Generating Capacity (Supplementary Investigation)
June 2011	Performance Audit: Flexible Work Arrangements for Public Employees
July 2011	Performance Audit: Dealing with Asylum Applications
October 2011	Information Technology Audit: Inland Revenue Department
November 2011	ARMS Ltd. – Setting Up and Operations
November 2011	Members of Parliament Honoraria
December 2011	Annual Audit Report of the Auditor General – Public Accounts 2010
February 2012	Performance Audit: Safeguarding Malta's Groundwater
March 2012	Performance Audit: Employment Opportunities for Registered Disabled Persons
April 2012	Information Technology Audit: Heritage Malta
April 2012	Performance Audit: Contract Management Capabilities across Local Councils
May 2012	Performance Audit: An Analysis of the Pharmacy Of Your Choice Scheme
June 2012	Performance Audit: Vehicle Emissions Control Schemes – Follow-up
June 2012	Public Broadcasting Services: Extended Public Service Obligation
July 2012	University of Malta Concession of parts of University House to the Kunsill Studenti Universitarji
July 2012	Information Technology Audit: Medicines Authority
August 2012	ARMS Ltd. – Follow-up
September 2012	Performance Audit: Tackling Problem Drug Use in Malta
October 2012	Procurement analysis through case studies 2007 to 2009
December 2012	Annual Audit Report of the Auditor General – Public Accounts 2011
December 2012	Performance Audit: Advertising Malta as a tourist destination - a case study of the Italian Market
March 2013	Performance Audit: Simplification of the Regulations in Structural Funds
April 2013	Enemalta Corporation Delimara Extension Implementation
May 2013	Performance Audit: Managing Public Service Recruitment
March 2013	Performance Audit: Simplification of the Regulations in Structural Funds
April 2013	Enemalta Corporation Delimara Extension Implementation
May 2013	Performance Audit: Managing Public Service Recruitment
June 2013	Information Technology Audit: Primary and Secondary State Schools
June 2013	Performance Audit: The management of elective surgery waiting lists

NAO Work and Activities Report

January 2013	Work and Activities of the National Audit Office 2012