N A O
National Audit Office
MALTA

# Information Technology Audit

## *Primary and Secondary State Schools*

**Report by the Auditor General** **June 2013**


# Information Technology Audit

# Primary and Secondary State Schools

# Table of Contents


**List of Abbreviations** 4

**Executive Summary** 6

**Chapter 1 - Introduction** 10

1.1 Background 10
1.2 Organisation Structure 13
1.3 Legislation 14
1.4 ICT in Primary and Secondary State Schools 14
1.5 Audit Scope and Objectives 17
1.6 Audit Methodology 18
1.7 Structure of the Report 18
1.8 Acknowledgement 19

**Chapter 2 - IT Management** 20

2.1 Background 20
2.1.1 eLearning Centre 20
2.1.2 Information Management Unit 22
2.2 IT Strategy 23
2.3 ICT Budget 24
2.4 Systems Development Life Cycle 26
2.4.1 Software Asset Management 26
2.4.2 Hardware Asset Management 27
2.5 PC Leasing Scheme 28
2.6 IT Inventories 29
2.7 Third Party Suppliers 31
2.8 Network Infrastructure 32

**Chapter 3 - IT Applications** 34

3.1 Educational Assessment Unit system 34
3.2 Oliver Library Management system (LMS) 36
3.3 eLearning Solution 42
3.4 TimeTabler system 46

**Chapter 4 - Information Security** 48

4.1 Security Management 48
4.1.1 Disposal of Information 48
4.1.2 Backup and Recovery of Data 49
4.2 Identity and Access Management 50
4.2.1 Authentication 50
4.2.2 Password Management 51

4.2.3 Information Access Control 52
4.2.4 Auditing 52
4.3 Security Awareness and Training 53
4.4 Anti-Virus Software 54
4.5 Patch Management 55
**Chapter 5 – IT Operations 56**
5.1 Security Controls 56
5.1.1 Physical Access Controls 56
5.1.2 Environmental Access Controls 57
5.2 Health and Safety Unit 58
5.3 IT Service Management 59
5.4 E-mail and Internet Services 61
5.5 Web Filtering 62
5.6 Risk Management 63
5.6.1 Business Impact Analysis 63
5.6.2 Risk Assessment 64
5.6.3 Business Continuity and Disaster Recovery Plans 65
**Chapter 6 – Management Comments 66**

**Appendix A – Organisation Chart 68**
**Appendix B – State Colleges 69**
**Appendix C – COBIT Controls 79**
**Appendix D – Restrictions on use of E-mail and Internet services 83**
**Appendix E – Business Continuity and Disaster Recovery Plan 85**

**Table 1 - ICT Budget allocated to State Colleges 24**

**Figure 1 - Student Population 12**
**Figure 2 - Geographical Map of the State Collages in Malta and Gozo 14**
**Figure 3 - eLearning Centre 22**
**Figure 4 - IT Inventory 29**
**Figure 5 - Library Resources 39**
**Figure 6 - Loans Statistics 41**
**Figure 7 - COBIT Controls 79**

# List of Abbreviations

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

| | |
|---|---|
| ADSL | Asymmetric Digital Subscriber Line |
| BCDR | Business Continuity Disaster Recovery |
| BCP | Business Continuity Plan |
| BDS | Bibliographic Data Service |
| BIA | Business Impact Analysis |
| CCTV | Closed Circuit Television |
| CD | Compact Disk |
| CdB | Common Database |
| CIMU | Central Information Management Unit |
| CIO | Chief Information Officer |
| COBIT | Control Objectives for Information and related Technology |
| DCMeL | Department of Curriculum Management and eLearning |
| DES | Directorate for Educational Services |
| DoS | Denial of Service |
| DQSE | Directorate for Quality and Standards in Education |
| DRP | Disaster Recovery Plan |
| DVD | Digital Versatile Disc |
| EAU | Educational Assessment Unit |
| ECDL | European Computer Driving Licence |
| eLC | eLearning Centre |
| e-mail | Electronic Mail |
| EO | Education Officer |
| eRFS | Electronic Request for Service |
| EU | European Union |
| GB | Gigabyte |
| GMICT | Government of Malta Information and Communication Technology |
| H&S | Health and Safety |
| HTTPS | Hypertext Transfer Protocol Secure |
| ICT | Information and Communication Technology |
| IMU | Information Management Unit |
| INSET | In-Service Training |
| IPSL | Industrial Projects and Services Limited |
| IT | Information Technology |
| ITSM | Information Technology Service Management |

| | |
|---|---|
| ITT | Invitation to Tender |
| IWBs | Interactive Whiteboards |
| LAN | Local Area Network |
| LMS | Library Management System |
| LPO | Local Purchase Order |
| LSA | Learning Support Assistant |
| MAGNET | Malta Government Network |
| Mbps | Megabits per second |
| MCA | Malta Communications Authority |
| MEDE | Ministry of Education and Employment |
| MEPA | Malta Environment and Planning Authority |
| MIS | Management Information System |
| MITA | Malta Information Technology Agency |
| MITC | Ministry of Infrastructure, Transport and Communications |
| MUT | Malta Union of Teachers |
| NAO | National Audit Office |
| OPAC | Online Public Access Catalogue |
| OPM | Office of the Prime Minister |
| PABX | Private Automated Branch Exchange |
| PC | Personal Computer |
| P2P | Peer-to-Peer |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SEP | Symantec Endpoint Protection |
| SIS | Schools Information System |
| SLA | Service Level Agreement |
| SLS | Schools Library Service |
| SMT | Schools Management Team |
| SQL | Structured Query Language |
| STS | Student Teachers' System |
| UPS | Uninterrupted Power Supply |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WSUS | Windows Server Update Services |

# Executive Summary

## Background

The National Audit Office (NAO) carried out an Information Technology (IT) audit in Primary and Secondary State schools within the State Colleges. The concept of the Colleges was proposed in 2005, with the aim that schools are networked together, so that children would attend a Primary school in their village or town and then proceed to a Secondary school within the same College.

The management and administration of State Colleges refer to the Education Act, which established a framework of decentralisation and autonomy of the educational operation. The Education Act also defines the services given by the Colleges and their schools according to the priorities, targets and national strategies adopted by the Government.

In 2009, all 10 Colleges were setup and placed in operation to cater for 31,910 students. To date, the student population in all 10 Colleges is divided into 5,608 Kindergarten students, 13,518 Primary School students and 12,784 Secondary School students.

The aim of this report is to collect and analyse evidence to determine whether State Colleges have 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.

Key Findings and Recommendations

Key issues addressed in this report (Chapter 2 refers) focused on how State Colleges are managing their IT resources, in terms of hardware and software applications, network infrastructure and supplier management.

a. In February 2012, a new Helpdesk function was setup within the eLearning Centre. The NAO noted that the eLearning Helpdesk do not register incoming calls in a Call Logging system. However, they are currently looking into the possibility of procuring a Helpdesk and IT Service Management software application to cater for the eLearning Solution.

b. The Ministry of Education and Employment (MEDE) does not have its own documented IT strategy. However, the MEDE refers to the *"National ICT Strategy for Malta 2008-2010"* also known as the "The Smart Island Strategy", which was launched by the Ministry of Infrastructure, Transport and Communications (MITC) together with MEDE. The NAO recommends that the MEDE draws up its own IT strategy, for the implementation of a number of initiatives, with the aim to achieve the strategic objectives highlighted in the National ICT Strategy.

c. The eLearning Centre manage all the leased PCs and Laptops, Interactive Whiteboards (IWBs) and projectors. To-date, the eLearning Centre handles 6,196-leased PCs, 4,210-leased Laptops, 2,573 IWBs and 2,573 projectors. Even though the eLearning Centre has a well-organised inventory process, the NAO recommends that the eLearning Centre should look into the possibility of providing a system whereby all the hardware inventory forms are registered electronically.

d. In terms of hardware asset management, whenever a laptop is taken for repairs, the user is not being provided with a temporary replacement and is sometimes left stranded without a laptop for months. The NAO noted that this shortcoming is mainly attributed to a Local Purchase Order (LPO), which is not issued on time by the department to replace a faulty part or the way in which insurance claims are being handled between a third-party supplier and their respective insurance firms.

e. The NAO noted that the eLearning Centre does not have sufficient hardware equipment to cater for any forthcoming projects or new posts within the State Colleges. The NAO recommends that the MEDE should liaise with the eLearning Centre in advance before personnel are allocated or new projects are scheduled.

f. The Government of Malta invested heavily to provide a robust and secure Wide Area Network (WAN) connection with the implementation of Fibre-Optic in most of the Primary and Secondary schools within the State Colleges. However, the NAO were informed that the network is heavily utilised using IWBs and the Internet during school hours. The NAO recommends that the MEDE commissions MITA to assess the impact of the increased Internet usage following the introduction of IWBs for future capacity planning.

The IT audit reviewed the four major software applications used within the State Colleges (Chapter 3 refers), in terms of ease-of-use, the security controls in place, account management and hosting services. The NAO notes with satisfaction that overall, all the four software applications reviewed in this IT audit are being managed effectively by the respective users. However, the NAO recommends that all the systems should ensure that access controls, in terms of password management, must follow the login and password security best practices. In this regard, the *'Remember me next time'* options should be immediately removed from any system, as this may compromise the confidentiality, integrity and availability of data if an unauthorised user gains access to the system.

# Executive Summary

This audit report also include (Chapter 4 refers) a review of the key components and the extent of Information Security measures that were implemented within the State Colleges, to maintain the confidentiality, integrity and availability of data.

a. State Colleges do not have or refer to an information classification policy or an information retention and storage policy. However, the NAO noted that State Colleges do take precautions on how to prevent the loss of any sensitive information from any of its IT equipment, in terms of disposal of information and backup and recovery of data.

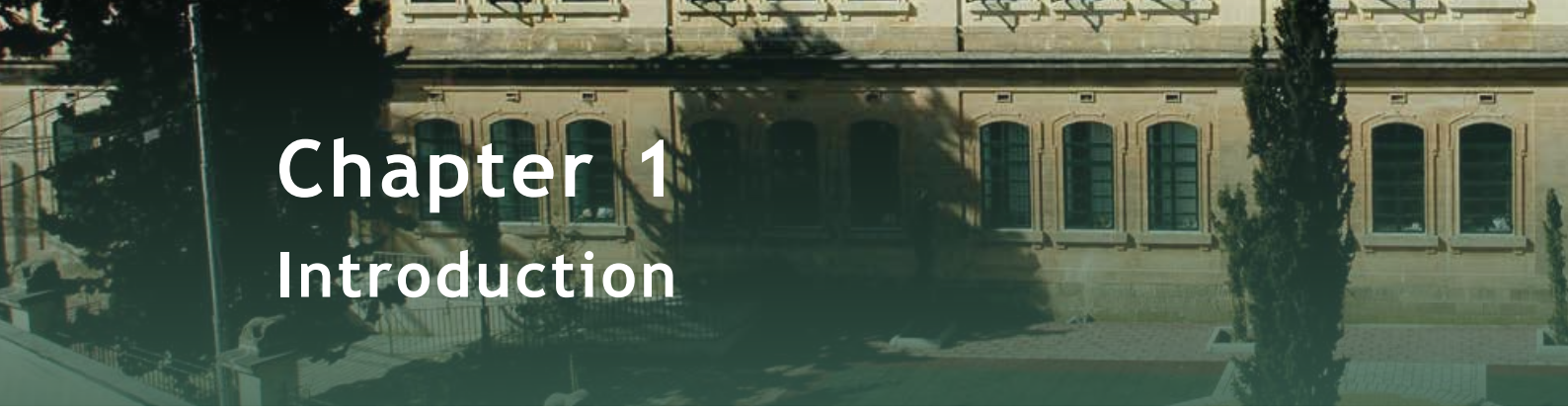
b. All the users who own a leased laptop should ensure that any personal information should be completely removed before the equipment, which is no longer in use, is returned to the eLearning Centre or transferred to another user. It is to be noted that all the laptops that are returned to the eLearning Centre are re-imaged. However, laptops that are transferred within a school are not re-imaged. Re-imaging then takes place if requested by the teachers themselves. The NAO recommends that any leased laptop should be securely wiped and re-imaged before the equipment is handed-in to another user, to ensure that there is no personal information or any hidden malware residing on the laptop.

c. The NAO notes with satisfaction that the Directorate for Educational Services and the eLearning Centre were involved in the *'BeSmartOnline!'* national project aimed at promoting the online safety of Maltese children and youth. The project was supported by the EU Safe Internet Programme, which aims at empowering and protecting children and young people when online, by supporting awareness-raising initiatives and backing the fight against illegal and harmful online content and conduct. The NAO recommends that similar initiatives be on going to instil security awareness in State Colleges.

The final component of the report (Chapter 5 refers) delved into the management and controls of IT operations to maintain data integrity and to ensure that the IT setup can successfully implement a disaster recovery process should the need arise.

a. The Physical and Environmental access controls in State Colleges are fundamental to ensure that the computer hardware, software and network infrastructure are protected from damage, theft and unauthorised access or from naturally occurring events such as lightning, flooding, fire, electrical interruption and other environmental disasters respectively. The NAO noted that the main networking cabinet were installed in confined areas or rooms normally used for the storage of boxes, or utilised by the school technician. In this regard, the school authorities should immediately remove any items that might pose a risk to the main networking cabinet, including clutter, storage of files etc. Furthermore, the NAO recommends that State Colleges should continue to invest in the physical and environmental controls in order to provide a more secure environment for the IT related resources within the Primary and Secondary State schools.

b. State Colleges do not have a formally documented business continuity and disaster recovery (BCDR) plan at a school level. On the other hand, the State Colleges' IT systems hosted at MITA, including the eLearning solution, are covered by a BCDR plan. The NAO suggests that the MEDE should perform a Business Impact Analysis and a Risk Assessment exercise in State Colleges on the basis of which a Business Continuity and a Disaster Recovery Plan can be drafted at a school level.



# Chapter 1
# Introduction

The MEDE invested heavily in the educational setup with the modernisation of State schools, the upgrading of the current network infrastructure and the provision of the latest IT equipment, with the introduction of IWBs, to offer an attractive learning environment to all students.

With the aim of improving the quality, standards, operation, initiatives and educational achievements in State schools, a new College system was established. All Primary and Secondary State schools now form part of 10 Colleges, nine in Malta and one in Gozo. This facilitated the transition from Primary to Secondary education with the introduction of the *"End of Primary Benchmark Assessment"* instead of the Junior Lyceum common entrance examinations.

In 2011, the MEDE reviewed the National Curriculum Framework and a new document, entitled *"Towards a Quality Education for all"* was published. This triggered an intensive and comprehensive consultation process among a number of stakeholders with the aim to promote:

- The development of lifelong learners who are engaged and responsible citizens, and active in the economy;
- The support for all learners to achieve and succeed, whatever their backgrounds, needs and aptitudes;
- A clear focus in Colleges and schools on meeting the needs of all learners through increased curricular economy.

After the consultation process, the National Curriculum Framework was officially launched on the 14th February 2013.

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

## 1.1 Background

The concept of the Colleges was proposed in the document entitled *"For All Children To Succeed"*, which was published by the MEDE in 2005, whereby the idea of networking schools together in Malta was first introduced. The proposal was for schools to be networked together in that children would attend a Primary school in their village or town and then proceed to a Secondary school within the same College.

Each school would have its own Head of school and employees. A College would comprise a network of these schools, having a College Principal chairing a council of Head of schools. The network would include a number of Primary schools that would lead students to the related Secondary schools within the College.

A pilot project was initiated in 2005, with the setup of the first three Colleges, namely St. Benedict, St. Margaret and the Gozo College.

In 2006, amendments were made to the Education Act and the concept of Colleges was enshrined in law. Each College was given a legal personality and the functions of the College and the College Principal were clearly laid out. Part V of the Education Act states amongst others that:

- *"Every College shall have a Principal who shall be the Chief Executive Officer of the College and who shall be responsible to the Directors General as regards to the performance of his functions and of the College according to respective issues, and to the College Board where matters are incumbent on the Board according to its functions"*

- *"Every College shall have a Board appointed by the Minister and which shall be composed of not less than five, but not more than seven members, one of whom shall be appointed as President. The members of the Board shall be appointed for three years provided that when the term of office of a member expires he may be reappointed for a further term of terms"*

- *"The College Board is a consultative Board, with the function of supporting the College, to acquire the services and the resources required for the implementation of its functions, and to monitor that these functions are being performed"*

- *"The Principal shall report regularly to the Board on the performance and operation of the College and point out any matter about which advice would be required to be given. The Board is entitled to request information about the functioning and the development of the College and the Principal is duty bound to procure the required data. The Board shall discuss the Business Plan and the Financial Estimates of the College prior to their presentation to the Directorates for their consideration. The Board shall contribute towards keeping the College close to the world of work, the economy, and the communities to which the students belong"*

Following the setting up of three Colleges in 2005, in 2009 all 10 Colleges were setup and placed in operation to cater for 31,910 students. As shown in Figure 1 below, to date, the student population in all 10 Colleges is divided into 5,608 Kindergarten students, 13,518 Primary School students and 12,784 Secondary School students.

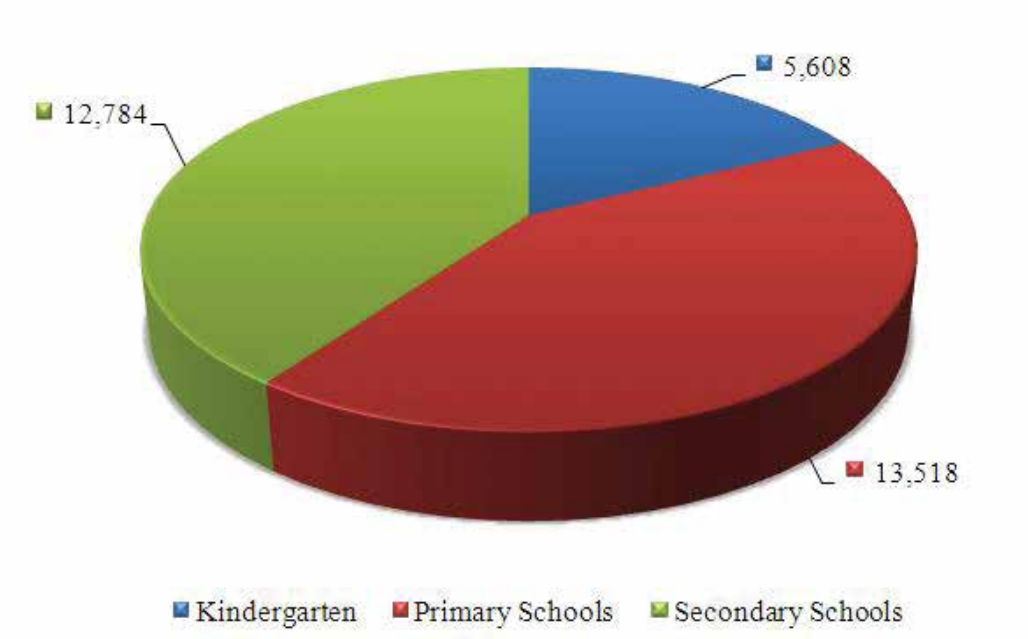



**Figure 1- Student Population**

Through the new College system there is an increased sharing of ideas, resources and experience and this has made the educational experience of professionals all the more richer when compared to the previous educational setup. Decisions are being taken closer to the grassroots, whilst the role of the Education Directorates is to set out frameworks of operation and policy.

According to the Education Directorates, the set up of the new College system was not an easy task. The biggest challenge was bringing people on board and instilling a new sense of ownership.

## 1.2 Organisation Structure

Following an amendment in the Education Act, between 2007 and 2008, the Directorates for Education went through a reform, which directly addressed the principle of subsidiarity in the management and administration of the State Colleges. The Education Act established a framework of decentralisation and autonomy of the educational operation and services given by the Colleges and their schools according to the priorities, targets and national strategies adopted by the Government.

In this regard, in November 2007, two Director Generals were appointed and entrusted with the responsibility of the Directorate for Educational Services (DES) and the Directorate for Quality and Standards in Education (DQSE) respectively. As depicted in Appendix A, both Directorates report directly to the Permanent Secretary of the MEDE.

The function of the DES is that of collaborating with the State Colleges and educational institutions, to plan, provide and allocate resources, and other ancillary support tools, and to encourage and facilitate their networking and co-operation.

On the other hand, the function of the DQSE is to regulate, guide, evaluate, verify, research and report on the various elements and the results of the compulsory education system with the aim of assuring quality education for all. Furthermore, the DQSE promotes good practices in all activities related to education as established in the national curricular framework of lifelong learning.

At the time of the drafting of this report, the Minister and Permanent Secretary's offices are located at 210, Strait Street Valletta, whilst both the Directorates were located at the Education Head Offices in Floriana. There is also an Education Centre in Victoria Gozo. As mentioned earlier, the State Colleges are dispersed geographically, namely nine Colleges in Malta and one in Gozo as depicted in Figure two.

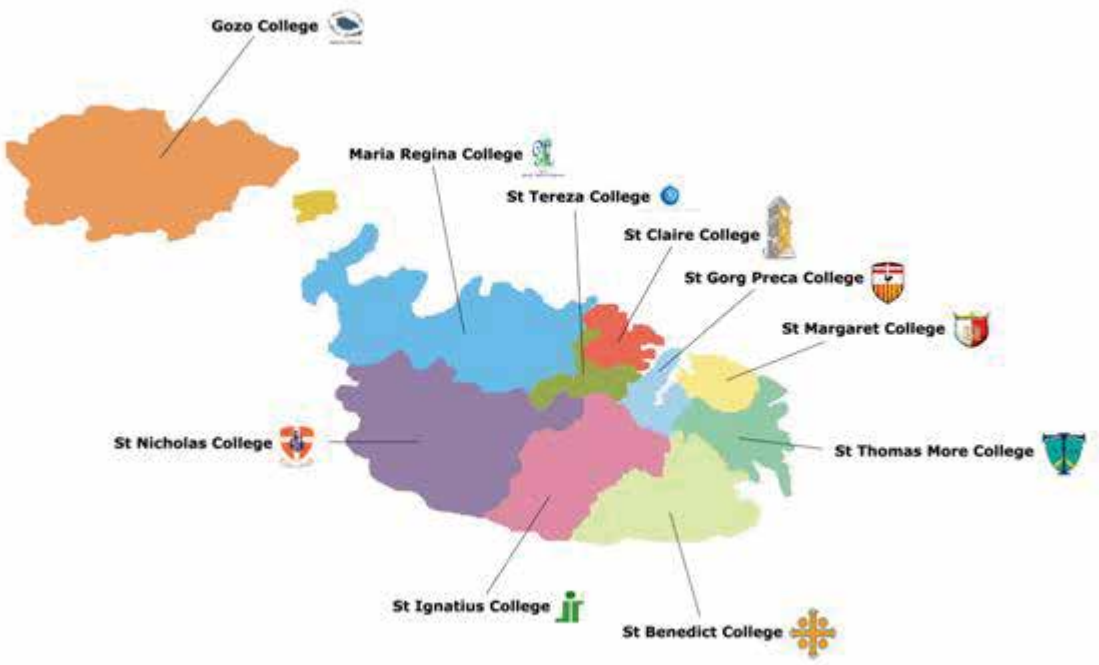



**Figure 2 - Geographical Map of the State Colleges in Malta and Gozo**

Furthermore, Appendix B lists all the Primary and Secondary schools within every State College.

## 1.3 Legislation

The State Colleges within the MEDE refer to the Education Act found in Chapter 327 under the Laws of Malta.

## 1.4 ICT in Primary and Secondary State Schools

Ever since the introduction of Information and Communications Technology (ICT) equipment in all Primary classrooms in 1996, to the current implementation of IWBs, an eLearning Solution and the continuous provision of educational software, ICT contributed to an increase in the quality and effectiveness of formal education.

Over the past 16 years, the Government invested heavily to provide a technical infrastructure within all State schools that delivers ICT capabilities to students and teachers. Personal Computers (PCs) and laptops were provided to teachers and State schools as part of the PC Leasing Scheme. Furthermore, the WAN connectivity in most of the Primary and Secondary schools was recently upgraded from an ADSL or Cable connection to Fibre Optic connection, to increase the bandwidth speed and provide a true broadband connection.

Apart from the number of educational software packages used in Primary school classrooms and Secondary school computer labs, the applications below are mainly used by the administration staff, teachers or school librarians within the College system.

- CdB (Common Database) online query – The Common Database is a central data repository used by authorised persons within the Government departments. The CdB provides access information about persons, addresses, organisations and the inter-relationships between these subjects found in the Public Domain. Thus, the information must be correct, consistent, up-to-date, and available at the right time and at the right place to better service the public.

- Educational Assessment Unit (EAU) system – The system manages the logistics for the End of Primary Benchmark Assessments. The aim is to notify the students and their parents or guardians, as well as the participating schools about the achievement of each student in the different skill areas of Maltese, English and Mathematics.

- eLearning Solution – It is a web-based learning environment that combines a broad range of ICT systems, including an eLearning platform and a Management Information System (MIS). The eLearning Solution is made up of:

    - e1 – Schools Management Information Systems – It is a system were leaders and administrators are able to manage and use learner and teachers' data more effectively.

    - iLearn Platform – It is a system that supports educators to upload and organise their lessons and resources as digital content in a repository. Content and resources can be shared with other colleagues and learners. Students will be able to access the work that the teacher assigns to them, whilst parents will be able to access their son's/daughter's results and assessments.

- e1 – Finance system – It is a fully integrated, double entry accounting package, which also includes an asset register module. In the next scholastic year, the e1 - Finance, will replace the current Schools Information System (SIS) Cash Accounts application used in State Colleges.

- Oliver Library Management system (LMS) – Oliver is a web-based library management system that delivers an innovative Library service to students and teaching staff.

- Outlook.com – It is a free, modern cloud e-mail service from Microsoft. As of July 2012, all the teachers' Government e-mail address (@gov) was replaced by Outlook.com (@iLearn.edu). The Outlook.com package also includes a free Word, Excel and PowerPoint built-in web applications together with a 7GB of free cloud storage for sharing photos, videos or other large files without huge attachments.

- SIS Cash Accounts – This application is used for the recording of the financial transactions in the respective school and for the eventual reporting of the expenditures to the Head Office. The SIS Cash Accounts is going to be replaced with the e1 - Finance system in the next scholastic year.

- TimeTabler – It is a fast and friendly computer application that is used within every Secondary school to schedule the school timetable quickly and accurately.

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

- Educational Assessment Unit system
- Oliver LMS
- eLearning Solution
- TimeTabler

## 1.5 Audit Scope and Objectives

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

The IT Audit was divided into three different stages:

- Initially, a pre-audit questionnaire was sent to the Information Management Unit (IMU) Office within the MEDE, to gather the necessary information on the audit site prior to undertaking an on-site audit. The aim of the questionnaire was to familiarise the audit team with the State Colleges and its IT setup prior to the audit visit.

- The second stage required a thorough understanding of the State Colleges internal structures, functions and processes through a number of interviews with key officials and stakeholders. The NAO also reviewed the draft National Curriculum Framework issued by the MEDE, user manuals and other documents requested in the pre-audit questionnaire.

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

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

- Gather all the relative information collected during the course of the IT audit.

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

- List all the findings and identify any potential risks.

- List all the recommendations to mitigate those risks.

## 1.6 Audit Methodology

To achieve these objectives, a number of interviews were held with Heads of School, the Chief Information Officer (CIO), Heads of Department, school clerks, the staff within the eLearning Centre and other officials. Furthermore, the NAO randomly selected a few Primary and Secondary schools from different Colleges in Malta and Gozo, to review the procedures of the different applications being used and the security measures that are being adopted to maintain the confidentiality, integrity and availability of data.

This audit report also refers to the Control Objectives for Information and related Technology (COBIT) set of best practices, which are listed in Appendix C. COBIT, is a comprehensive set of resources that contains all the information organisations need to adopt IT governance and control framework. COBIT provides good practices across a domain and process framework in a manageable and logical structure to help optimise IT-enabled investments and ensure that IT is successful in delivering against business requirements.

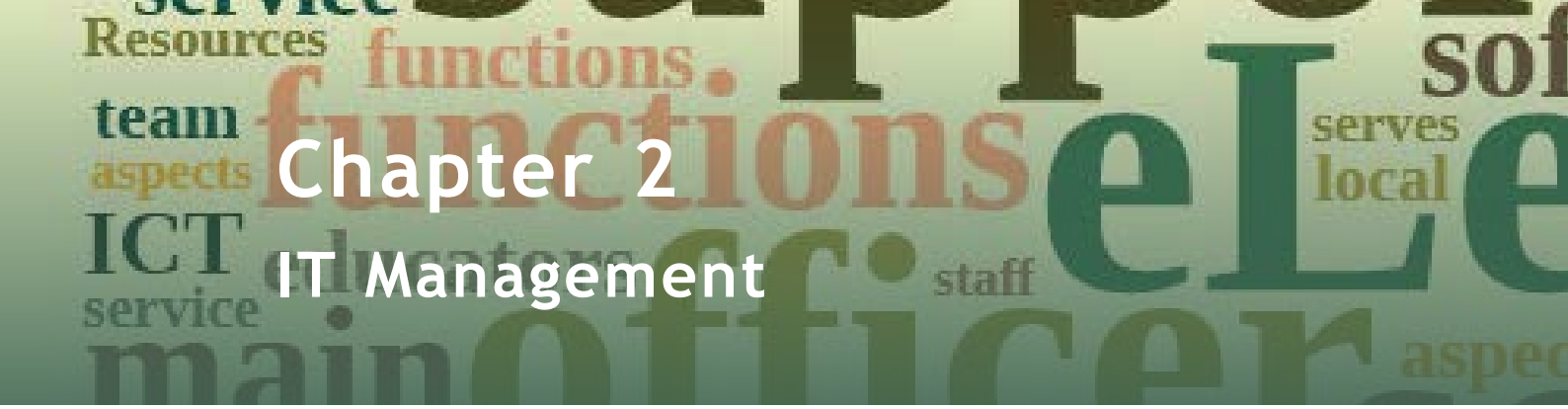
## 1.7 Structure of the Report

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

- Chapter 2 deals with the IT management and whether technology resources are managed in accordance with its needs and priorities.
- Chapter 3 reviews a selection of IT applications that are currently being used within the State Colleges.
- Chapter 4 addresses the key components of information security and which security measures were implemented within the State Colleges, to maintain the confidentiality, integrity and availability of data.
- Chapter 5 analyses how State Colleges are managing and controlling their IT operations in the most effective way. Furthermore, it addresses whether State Colleges are confident with any business continuity or disaster recovery plans in the event of a service disruption.
- Chapter 6 lists all the management comments.

## 1.8 Acknowledgement

The NAO would like to express its thanks and appreciation to all the staff within the MEDE, in particular the CIO, Directors General, Heads of Department, Heads of School, the eLearning Centre and all other officials who were involved in this audit, for their time, patience and assistance.




# Chapter 2
# IT Management

## 2.1 Background

The ICT in Education unit forms part of the eLearning Centre within the Department of School Resources, falling under the responsibility of the DES. Before 2007, the unit was being managed by a CIO, who was in charge of all the ICT in schools. When the CIO retired, the unit was being managed by a number of Education Officers (EO) until a Service Manager within the unit was appointed in March 2009. Even though the Service Manager reported directly to the Department of School Resources Management, the Service Manager was also assigned to the DQSE, under the guidance of the Director of the Curriculum Management and eLearning Department and the Director General for Quality and Standards in Education. The Service Manager's main responsibility was the management of the eLearning Centre.

In August 2012, the Service Manager was re-appointed again under the DES. In the meantime, the DQSE issued a call for an Assistant Director for eLearning, who was then assigned to the post in October 2012. To-date, both the Service Manager and the Assistant Director for eLearning are responsible for the smooth running of the eLearning Centre.

### *2.1.1 eLearning Centre*

The eLearning Centre has a number of functions within the Department of School Resources. It serves as the main support office on ICT for educators and offers support on various aspects related to ICT.

The eLearning Centre has a staff compliment of 82 personnel, which includes the Service Manager and the Assistant Director. As depicted in Figure three the 24 Support Teachers at the eLearning Centre fall under the responsibility of the Service Manager together with six officers within the Network team. The latter consists of one Senior Technical Officer in charge of four IPSL (Industrial Projects and Services Limited) personnel and one officer, responsible for any works/issues related to the local network infrastructure in schools. The Network team currently has one IPSL personnel on prolonged leave. There are also five ICT technicians, namely two ICT technicians in charge of the Gozo College and three ICT technicians in charge of all the remaining nine Colleges in Malta, one Art/Graphic technician, and one Learning Support Assistant (LSA). The Service Manager is also responsible for one teacher on office duties working with the Support teachers, and one General Hand, who has a technical background and performs technical work.

The technicians perform various works in State Colleges. Amongst others, they scan and test new network connections in schools, activate networking points and are


responsible for the logistics of IWBs. Whenever an IWB needs to be re-allocated, lowered or tested for network connectivity, the respective school contacts the Service Manager through an e-mail, who will then assign the job to the technicians according to priority.

On the other hand, there are two Educational Officers (EOs) and another three EOs that are still vacant. The 20 Primary eLearning Support teachers and 12 Secondary eLearning Support teachers, whose work is to support teachers in schools with the use of technology and the methodology to be used, together with two Support teachers in charge of the eTwinning[1], fall under the responsibility of the Assistant Director eLearning.

The Primary and Secondary eLearning Support teachers meet once a week at the eLearning Centre to share ideas and raise any issues they might have encountered during the week, while the Support teachers based at the eLearning Centre meet once a month with the Service Manager, to discuss the various ongoing tasks.

The Support teachers cater for Graphic Design and Publications, the update of an online database called *'The Asset Management System'*, where all leased equipment are listed, together with an internal database were all the transfer of assets are inputted. The Support teachers are also involved in the organisation of the European Computer Driving Licence (ECDL), both for pupils in schools and for teachers attending voluntary evening or summer courses, the organisation of Summer and Winter courses and all the logistics of EMBED[2]. A few Support teachers at the eLearning Centre provide support through the Helpdesk on the iLearn e-mail accounts and the iLearn platform, and support teachers through Microsoft application projects.

The eLearning Centre also consists of one Principal, an Assistant Principal (who works on Teleworking), an Executive Officer (who works on reduced hours) and two clerks who work with both the Service Manager and the Assistant Director.

There are also two Helpdesk officers, who are not counted for in the above. These Helpdesk officers are third-party contract employees, who fall under the responsibility of the Service Manager while on duty at the eLearning Centre. There is also a Helpdesk at the Schools Information System (SIS) section, which is located in a Secondary school within the State Colleges. The SIS Helpdesk provides support on e1 – Schools Management Information System. The latter is used by clerks and administration personnel.

[1] Reference: http://etwinning.skola.edu.mt/
[2] EMBED is an annual event were workshops are organised and pupils do hands-on experience.

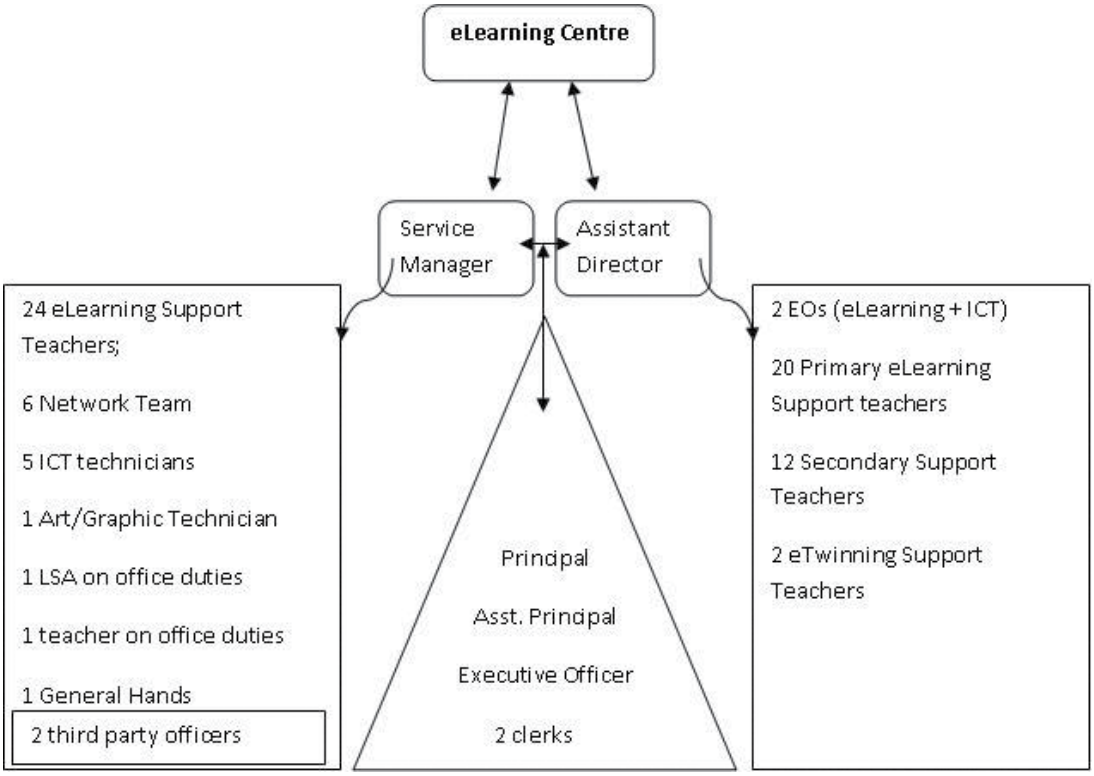




**Figure 3 - eLearning Centre**

The NAO observed that to-date, both Helpdesks do not register incoming calls in a Call Logging system. The eLearning Centre can only measure the amount of phone calls registered through the PABX but they cannot quantify the type of calls that are being handled by the Helpdesk function. However, the NAO were informed that the Directorates are currently working on issuing a tender for the procuring of an IT Service Management Application.

During the course of this IT Audit, the NAO observed that all the units within the eLearning Centre continuously interact with each other. Furthermore, a number of meetings are held on a daily basis through the different stakeholders.

### *2.1.2 Information Management Unit*

The IMU is the primary ICT business driver of the MEDE. The unit is made up of the CIO, an Information Management Systems Officer, a Contract and Services Officer, an Applications Officer and two clerical staff. The IMU champions consolidation within the Ministry, contributes to the development of corporate Ministerial ICT and e-Government policies and strategies.


The IMU is the primary interface of the Ministry with MITA. The latter provides the Ministry with core services such as e-mail and Internet, effects monitoring and compliance facets of ICT governance function, and advises the IMU about primary technology and ICT operations.

## 2.2 IT Strategy

As the MEDE does not have its own documented IT strategy, both the DES and DQSE follow the *"National ICT Strategy for Malta 2008 - 2010"*[3], also known as the *"Smart Island Strategy"*, which was launched by the MITC together with the Ministry of Education and Employment.

The *"Smart Island Strategy"* is based on the 2004 National ICT Strategy, which mapped out the country's consolidation steps in the global ICT scenario, soon after the eMalta Strategy, had put in place the basic building blocks for the attainment of the first-class information society and economy.

The *"Smart Island Strategy"* was constructed on five strategic parameters, which serve as the policy boundaries determining the ground on which the strategy is mapped out. Within the context of these five parameters, the *"Smart Island Strategy"* is a complex web of inter-twined initiatives constructed through a simple traditional 'hub-and-spoke' model, with the vision serving as the hub and seven inter-related strategic streams as spokes:

1. Robust ICT Environment and next generation infrastructure;
2. A connected society – bridging the last and the new miles;
3. Develop human potential into a smart workforce;
4. e for everything – enhancing Maltese citizens' quality of life through ICTs;
5. Re-inventing Government – transformation and open Government;
6. Taking Care of (e) Business;
7. Developing a world-leading ICT industry.

Each strategic stream features key strategic targets and is composed of a series of supporting spokes. The deployment of the spokes is supported by a structured set of strategic programmes and initiatives aimed at delivering the necessary contribution towards the attainment of the vision.

The measures set out in the *"Smart Island Strategy"* were intended to cover both Malta and Gozo. However, in each strategic stream a set of measures were specifically aimed at enhancing the relevance and strategic value of the Government's programme in the Gozitan context by emphasising the creation of the necessary infrastructure for

[3] Source: http://www.ictmalta.org.mt/category/content/strategies/national-ict-strategy


ICT education and take-up of opportunities in this sector. The Government believed that Gozo is an ideal location for the nurturing of pure knowledge-based industries and ICT-driven research and development activity. Each policy measure, programme or initiative will have a 'Gozo Dimension' added to it, making it fit in the wider landscape of promoting Gozo as an investment location.

Beyond the value of the programmes and initiatives, set out herein, the "Smart Island Strategy" is a cornerstone of Government's 2015 vision of transforming Malta, amongst others, in a centre of excellence of ICT. The attainment of its constituents by all the relevant stakeholders will certainly go a long way in realising this vision.

The NAO recommends that the MEDE draws up its own IT strategy, for the implementation of a number of initiatives, with the aim to achieve the strategic objectives highlighted in the National ICT Strategy.

## 2.3 ICT Budget

During the course of this audit, the NAO reviewed the ICT Budget allocated to State Colleges for 2011 and 2012, but this excludes the MITC allocation for the eLearning program. As documented in Section 2.7 of the report, the IT services provided by MITA are covered by a Ministry contract and not a contract specific to the State Colleges. Thus, the ICT Budget for 2011 and 2012, as depicted in Table 1 below, does not include the cost of leased PCs and laptops, IWBs and projectors, and the cost of IT support paid to MITA.

| ICT Budget | |
|---|---|
| 2011 | € 669,447 |
| 2012 | € 763,463 |

**Table 1 – ICT Budget allocated to State Colleges**

The NAO noted that in 2011, a substantial amount was utilised for the procurement of hardware for EOs, teachers and eLearning Support teachers, and educational software for both Primary and Secondary schools. A number of repairs on ICT assets were carried out and TV licences renewed. Furthermore, the network infrastructure was extended in a number of Primary and Secondary schools and some alarm systems underwent maintenance in schools. Funds were also allocated for the organisation of the annual EMBED event and for the procurement of Skills Cards. The latter provide an alternative teaching method of practising the key skills in a particular subject. They are normally used by teachers, who are attending evening and summer courses.


Similiarly, in 2012 a substantial amount was used for the procurement of hardware and educational software, hardware repairs and to expand an existing network infrastructure in schools. A number of PCs and laptops were re-imaged with Windows 7 Operating System. Additional IWBs pens were procured and new hardware for children with special needs was provided in schools. Furthermore, security measures were enhanced with the installation of intruder alarms in certain schools.

Apart from the above expenses, the NAO observed that every school manages two different funds, namely the Imprest Funds and the School Funds. Whilst the Imprest Funds are allocated by the Ministry according to the type of school (Primary or Secondary) and the schools' student population, the School Funds are raised by the school council through fund-raising activities, the sale of objects produced by students or from the renting of school premises after school hours.

The Imprest Funds are classified under three different line votes, namely Capital Expenditure Equipment, Materials and Supplies, and Maintenance. The Capital Expenditure Equipment covers all items that can be described as equipment, such as Sports, Health and Safety or Science equipment and for the embellishment of the school premises with the installation or replacement of furniture, blinds or curtains etc. The Materials and Supplies covers all expendable items that need to be constantly replaced, including telephone bills and other mandatory fees, the procurement of milk, laboratory and workshop expendables such as chemicals, wood, poster colours, and consumables such as printer toners, ink cartridges and stationary. Finally, the Maintenance vote covers the repairs or alterations required within the school premises, such as the fixing of leaking pipes and water fittings, plastering, fixing of glass panes, locks or school furniture. At the end of the year, every Head of School must provide the Ministry with a detailed account together with the original fiscal invoices of all the expenses incurred under each vote. Furthermore, all unspent funds are to be returned by means of a cheque addressed to the DES.

On the other hand, the Head of School utilises the School funds whenever a school wishes to refurbish a particular room within the school premises, procure any hardware, which is not part of the PC Leasing scheme, such as a printer or photocopier, or procure new books for every classroom or school library in primary schools.


## 2.4 Systems Development Life Cycle

The IT Audit reviewed the systems development life cycle used by the MEDE, in terms of the processes involved in the planning, development, acquisition, testing, implementation and maintenance of software applications and the procurement, maintenance and disposal of ICT hardware equipment within the State Colleges.

### *2.4.1 Software Asset Management*

During the course of this IT audit, the NAO reviewed the project life cycle in terms of the software asset management. The NAO observed that every application in use within the State Colleges is either off-the-shelf software or a legacy systems upon which only a few enhancements were made.

The NAO has thus reviewed the project life cycle that is being followed within the eLearning Centre and IMU, whenever new software is procured or enhancements are applied on any existing software application.

In this regard, the NAO were informed that two different Invitations to Tender (ITT) for the *'Procurement of digital content and authoring tool for the Primary and Secondary Education Sector including the integration to the local e-Learning platform'* were recently issued by the DQSE. Bidders were required to provide interactive digital lessons, based on the Maltese Primary or Secondary school curriculum, with the scope of enhancing the teaching and learning processes, and in line with emerging pedagogies highlighted in the National Curriculum Framework. The ITT states that since the digital content procured within this tender will not cover the entire curriculum, teachers should be given the possibility to create their own digital learning objects. In this regard, the eLearning authoring tool will allow teachers to create their own digital learning objects. The NAO was informed that the tendering process is currently underway.

The NAO observed that the eLearning Centre are adopting a similar approach to the software project life cycle in both ITTs, which include:

- Feasibility study;
- Procurement of system requirements;
- Drafting of a conceptual design;
- Systems development;
- Systems testing;
- Implementation and
- Systems maintenance and support.


In 2012, the eLearning Centre went through most of the above-mentioned phases before all the leased PCs and laptops were re-imaged with Windows 7 Operating System and Microsoft Office 2010. Prior to all this, rigorous testing was carried out within the eLearning Centre to check on the compatibility of the existing educational software and to verify that there are no performance issues on any PCs or laptops, with the new Windows 7 Operating System. The same procedure applies whenever additional educational software applications are introduced in State Colleges.

The NAO were informed that a few State Colleges procured off-the-shelf software applications for their own use. However, this is not the norm. All the educational software applications are procured centrally and managed within the eLearning Centre. The latter keeps track of any educational software licences and holds an inventory[4] of all the educational software applications currently installed in State Colleges. On the other hand, the IMU procures all Microsoft software applications through MITA, as part of the Microsoft Enterprise Agreement. The IMU manages all these software licences and any other corporate software licences used within the State Colleges and Ministry.

The NAO recommends that if any software is to be procured by the State College (not procured centrally), a business case must be raised with the IMU before any commitment is made. The IMU together with MITA has to evaluate the impact of such a purchase on the existing ICT infrastructure.

### *2.4.2 Hardware Asset Management*

As detailed in Section 2.5 of the report, all State Colleges liaise with the eLearning Centre for the procurement of most of its IT equipment through the PC Leasing Scheme. Other IT equipment, which may be needed by the respective school, but is not covered under such an agreement, is procured through the imprest or school funds.

Since all State Colleges opted for the procurement of PCs and laptops through the PC Leasing scheme, all the old PCs and laptops used within the State Colleges were removed by the third-party supplier as per the PC Leasing agreement. The NAO were informed that all the Hard Disks residing on the pre-leasing IT equipment were wiped when the hardware was handed over to the contractors.

Peripherals, such as printers, scanners and photocopiers, are being maintained by the related third-party supplier. Any faulty hardware equipment, which is not part of the PC Leasing Scheme, must be certified in writing by the third-party supplier. The respective school will then inform the eLearning Centre accordingly. A board, made

[4] Refer to Section 2.6 – IT Inventories


up of a Principal and two other members from the eLearning Centre, will then visit the school to ensure that the equipment is faulty, before they certify it for disposal.

## 2.5 PC Leasing Scheme

In 2008, the Government of Malta through the MITC, embarked on the implementation of a PC leasing framework within the Public Service. The objective of this initiative was to have a more efficient and effective ICT service by implementing a programme entailing the replacement of existing equipment through the deployment, under title of lease of PCs and laptops, as well as for the provision of maintenance and support services to all workstations across the Public Service.

State Schools were amongst the first to adopt the PC Leasing Scheme whereby all the existing ICT equipment installed in Primary school classrooms, Secondary school computer labs and administration offices were replaced with leased PCs and laptops. Furthermore, Resource Centres and School Libraries were also included in the Government's PC Leasing Scheme. Most of the requests related to maintenance and repairs, are handled by MITA's Service Call Centre and all the calls are serviced by the respective third-party suppliers who were awarded the tender.

The NAO observed that every teacher, EO, psychosocial support staff, Head and Assistant Head of Schools, with the exception of the clerical staff, the LSAs and Kindergarten Assistants, within all the Primary and Secondary schools were provided with a laptop or a PC. Although the PC Leasing Scheme brought a number of benefits, both the NAO and the MEDE acknowledge that this scheme has also created a number of risks and limitations.

During the course of this IT Audit, the NAO observed that a number of concerns were raised by various users and Heads of sections on the overall running of the PC Leasing Scheme within the State Colleges. Whilst the overall level of support being offered improved drastically, a number of issues should be taken into consideration in the next PC Leasing contract.

Primarily, if a laptop is taken for repairs by the third party supplier, the user is not being provided with a temporary replacement. In this regard, sometimes teachers were left stranded without a laptop for months either because the supplier had to wait for a reply from the insurance firm or because the LPO was not issued on time by the department to replace a faulty part.

Secondly, when the PC Leasing contract was introduced in 2008/2009 scholastic year, the Ministry procured an 'X' amount of PC's and laptops to cater for the existing posts within the State Colleges. During the course of the PC Leasing term, the eLearning Centre responsible for the management of the PC Leasing equipment had a few

amount of leased equipment to cater for new posts within the State Colleges or to be used for any forthcoming projects. In this regard, the NAO recommends that the Ministry should inform the eLearning Centre in advance to ensure that adequate resources are available before new posts for the recruitment of personnel are issued or for any forthcoming projects.

The NAO noted that the laptop batteries are not included in the current leasing agreement. The NAO recommends that laptop batteries, and the laptop weight should also be taken into consideration when selecting new equipment for State Colleges.

## 2.6 IT Inventories

The NAO acknowledges the fact that the Schools Inventory Section, within the eLearning Centre, is responsible of keeping track all the leased laptops, PCs, IWBs and projectors in State Colleges. As depicted in Figure 3 below, to-date, the Schools Inventory Section handles 6,196-leased PCs, 4,210-leased laptops, 2,573 IWBs and 2573 Projectors.

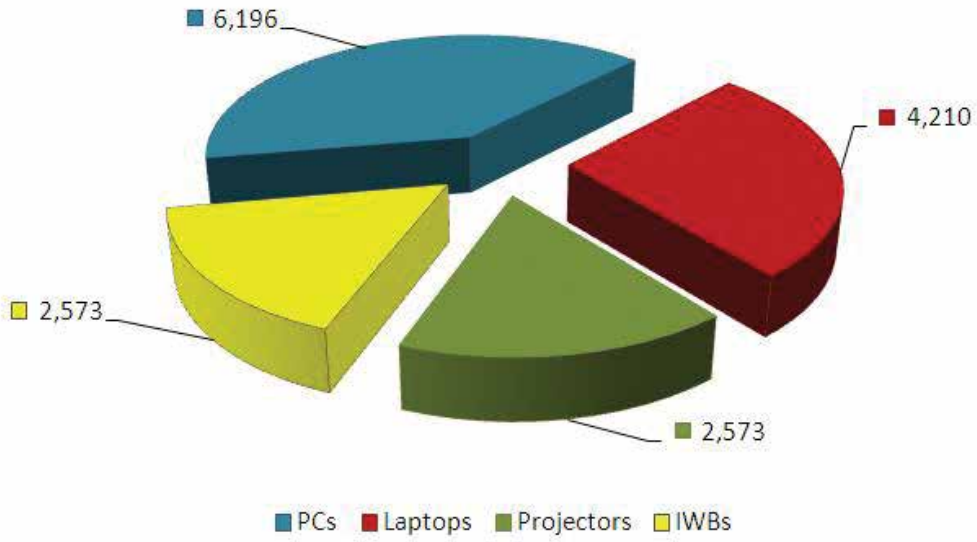



**Figure 4 – IT Inventory**

In the beginning of every scholastic year, the eLearning Centre sends an updated inventory list to every Primary and Secondary schools, which will include the inventories of all leased PCs and laptops, Projectors and IWBs. The schools' inventory list is normally maintained by either the Assistant Head or Computer Lab technician, who ensures that every piece of hardware is still in place and still owned by the same user.


To ensure that the schools' inventory list is kept up-to-date, the eLearning Centre issued four different hardware inventory forms:

- Form A should be filled in for teachers who retire, resign or avail of leave (such as parental, maternity, study, responsibility). This is necessary to prove that the person in question is returning the laptop at school in good working order. Form A is filled in, signed and a copy is given to this teacher, a copy is kept for the school records and the original is sent to the eLearning Centre.

- Whenever a laptop is returned and Form A is filled in accordingly, the laptop is then passed on to a teacher pending a laptop at the same school or centre if applicable. In this case, a Form B is to be filled in. A copy is kept for the school records and the original is sent to the eLearning Centre. If the laptop in question was not upgraded to Windows 7, then the teacher, who will be in possession of this laptop, must e-mail a request to reimaging@ilearn.edu.mt and fix an appointment with the eLearning Centre to upgrade laptop with the latest Operating System. If, on the other hand, the laptop has already been upgraded, then, Form B would suffice.

- If on the other hand, a teacher does not own a laptop and no laptops are available from within the same school, a request is sent to the eLearning Centre through Form C. This form is to be filled in for every teacher, signed by the Head of School and bearing the school stamp. As soon as the laptops are available, the teachers are informed to pick up their laptops from the eLearning Centre.

- Form D is to be filled in whenever laptops returned at school, are not passed on to teachers pending a laptop (Form B). In this case, instead of laptops lying idle in schools, a Form D is sent to the eLearning Centre. As soon as it is received, eLearning personnel are sent to collect the laptop/s concerned. Laptops brought over from schools to the eLearning Centre, can be then passed on to other teachers awaiting a laptop after re-imaging.

Apart from the above forms, the eLearning Centre has two other forms, which are used whenever a laptop is brought over for re-imaging purposes, namely the *"Laptop Inspection Details form"* and the *"Declaration of Asset Loaned form"*. The former is filled in by the technician from the eLearning Centre upon inspecting the laptop brought in for re-imaging. It lists a series of faults or damages, which could occur to a laptop. If any of these faults or damages is found, the technician will highlight them in the form. The latter ensures that the laptop is returned to the user in the same condition before the laptop was handed in for re-imaging. On the other hand, the *"Declaration of Asset Loaned"* is a form on which the teacher signs upon when he or she picks up the laptop from the eLearning Centre.


A different inventory form is used whenever Projectors and IWBs are moved from one school to another. The form must include both MITA and Education Inventory Numbers, the School Name and the Room number where the IWBs and Projector were removed and the School Name and Room number where the IWBs and Projector will be installed.

A similar procedure is applied on leased PCs. If a PC is transferred from one school to another, a form must be filled in, which must include the Make, Model, Serial Number, and Desktop Inventory number of both the PC and Monitor. The person in charge of the respective schools' inventory must fill in his or her Name and Surname, ID card number, Contact number, Signature, and the School and College names. Finally, the form must be signed by the Head of School and endorsed with the School rubber stamp. The original form is kept by the school and a copy is sent to the eLearning Centre.

On the other hand, whenever a PC is no longer needed, the Head of School must fill in a different form. All the details submitted in the above form, must be included in this form. Once the form is signed by the Head of School and endorsed with the School rubber stamp, the original copy is kept by the school and a copy is sent to the eLearning Centre. The latter will then pick up the PC from the respective school.

As mentioned earlier, the eLearning Centre keeps track of all the educational software licences and holds an inventory list of all educational software applications currently installed in State Colleges. Taking into consideration that the eLearning Centre, is manned by only four personnel, the NAO observed that the schools' inventory process is very well organised. However, the NAO recommends that the eLearning Centre should look into the possibility of providing a system whereby all these hardware inventory forms are registered electronically.

## 2.7 Third Party Suppliers

In line with the Office of the Prime Minister (OPM) Circular No. 29/2005, MITA being the ICT Agency for the Government of Malta, was entrusted with the provision of all Core Services to all Government and Public Sector entities.

All State Colleges have a Ministry wide contract with MITA that covers the Core Service items common to Government. In this regard, MITA provides the State Colleges with a Fibre-Optic, Cable or ADSL connection to the Government Network also known as MAGNET. The ICT services contract also covers the 24/7 monitoring carried out on the MAGNET, namely on core WAN equipment and Core Access Switches to prevent potential ICT problems resulting in service downtime. Furthermore, MITA is also providing State Colleges with a number of services:


- Hosting of Server Services and any Guest Virtualised Machine in a segregated environment;
- Standard Desktop Security Configuration Services, such as Anti-Virus and Patch Management;
- Access to MITA's Service Call Centre for the reporting of incidents related to the above services;
- First line support for the resolution of incidents, reported to MITA's Service Call Centre regarding the above-mentioned services to leased workstations.

State Colleges also utilise third-party suppliers for the repairs of non-leased items, such as printers, scanners or photocopiers. All the scanners and printers are maintained by two different third-party suppliers, through MITA's Service Call Centre. On the other hand, the school will contact the third-party supplier directly, whenever a photocopier requires maintenance. Since these suppliers are not bound with any Service Level Agreements (SLAs), the NAO recommends that State Colleges should at least come to an agreement with the respective third-party supplier, in terms of service response and repairs.

Both the IMU and the eLearning Centre ensures that all the third-party suppliers are offering a good level of support and abide by the terms and conditions stipulated in the maintenance contracts, especially when it comes to delivery dates and call-out rates were applicable.

## 2.8 Network Infrastructure

Almost all State Colleges are connected to the MAGNET, via a 10 Megabits per second (Mbps) Fibre-Optic link to MITA-01 Data Centre in St. Venera. Currently, MITA is in the process of converting a few remaining schools from an ADSL or Cable connection to an existing Fibre-Optic connection of a neighbouring school. However, MITA informed the NAO that a few schools or Education Centres would remain on Cable or ADSL connection, since most of these schools will be closing down in the near future or according to MEDE it is not feasible to connect them to a Fibre-Optic connection.

As part of the Core Services contract, all WAN equipment and Core Access Switches are monitored by MITA on 24/7. The network connectivity is monitored and maintained by MITA. The Head of School or school clerk is notified by MITA whenever there is a service disruption. Furthermore, whilst the LAN infrastructure is monitored by MITA, the eLearning Centre maintains the LAN infrastructure. In this regard, whenever there is a problem on the LAN infrastructure, the school will report the fault immediately to the eLearning Centre


As part of this audit, the NAO requested a network diagram of the schools' network infrastructure. In return, MITA provided the NAO with physical and logical network diagrams of the schools and eLearning infrastructure. In the meantime, the NAO visited a few Primary and Secondary schools, which were selected randomly from the existing Colleges. While reviewing the network setup, the NAO observed that most of the network cabinets are properly maintained and kept secure. However, since these network cabinets are installed in corridors, administration offices, computer labs or a dedicated room, which is commonly used as stores, the NAO recommends that every school should ensure that the network cabinet is not being obstructed with any furniture or piles of boxes. Furthermore, all cabinets should always be locked and keys are kept secured and only accessible by authorised personnel.

The NAO were informed that even though the Government has invested heavily on the WAN infrastructure, with the implementation of Fibre-Optic in most of the Primary and Secondary schools, the network is heavily utilised using IWBs and Internet connection during school hours. Thus, the NAO recommends that the MEDE commissions MITA to assess the impact of the increased Internet usage following the introduction of IWBs for future capacity planning.

# Chapter 3
# IT Applications

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

- Educational Assessment Unit system
- Oliver LMS
- eLearning Solution
- TimeTabler system

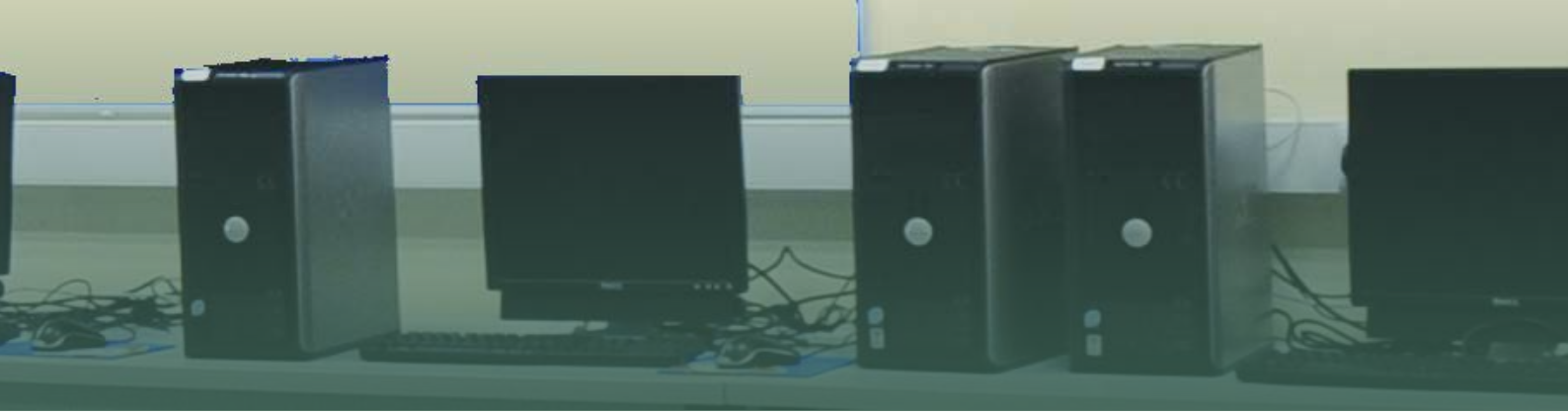
## 3.1 Educational Assessment Unit system

The EAU system is used by the DCMeL to manage the logistics for the End of Primary Benchmark Assessments. The first session of the End of Primary Benchmark Assessment was held in June 2011. These assessments replaced the long established Junior Lyceum and Common Entrance Examinations, which were used to determine the student's eligibility for a particular type of Secondary school. The aim of this assessment is intended to inform the students and their parents or guardians, as well as the participating schools about the achievement of each student in the different skill areas of Maltese, English and Mathematics.

The EAU system is a web-based application with a Microsoft SQL back-end and is only accessible within the DCMeL through an HTTPS connection. All the users attended training sessions and provided with a user manual, which is updated and maintained by the local supplier. In this regard, the NAO noted that personal information was extracted from the system and included in the manual as a sample report. The NAO recommends that this information is removed completely or replaced with fictitious data.

Following the above recommendation, the NAO was informed that the local supplier took immediate action, whereby the personal information was removed completely from the user manual and replaced with fictitious data. Furthermore, the manual report was updated to a newer version while the previous version manuals used internally were destroyed.

The EAU system has two different user levels, namely the administrator and the end-user level. While the latter has read-only access, the administrator manages all user accounts and can delete records or data at the application level. Data is provided by school clerks who are also responsible to maintain a pre-defined template with all students' information, which include ID card number, name, surname, gender, home address, their respective parents or guardian names, school name, class and the subjects undertaken in a specific scholastic year. All the data is saved in .CSV format and sent to the EAU system administrator who will then import all the information into



the database. If minor changes are required, these are normally inputted manually by the administrator. Once student data has been imported or inputted manually, the system will generate a code and office number for every student. These codes will then trigger an alert if a student has already been assigned a code or a duplicate entry is detected in the system.

The EAU system has a Security module, which allows an administrator to create and maintain user accounts. The Security module gives the administrator the functionality to control the information, define different groups, add users to a group and assign permissions to a group. The NAO noted that audit trails are in place to record any amendments or deletions made on the system.

The EAU system is controlled by a username and password. Password complexity rules are enforced and all passwords expire after a specific period. Old passwords cannot be re-used after expiry and the system will block access after three unsuccessful attempts. The NAO observed that the login page has a *"Recover Password"* option, which will allow the user to request a forgotten password. Furthermore, the user can also click on the *"Remember me next time"* checkbox to save the user credentials. If the checkbox is selected, the user will either be logged in automatically or else will have the credential fields automatically populated when accessing the system. Unfortunately, the *"Remember me next time"* option is against the security login principles, as this may compromise the confidentiality, integrity and availability of data if an unauthorised person gains access to the system. In this regard, the NAO recommends that the *"Remember me next time"* option is removed completely to prevent any misuse of the system and the password expiry is lowered from the current time window.

In addition to the standard reports provided by the system, the NAO observed that the administrator could also create different ad-hoc reports through the SQL Server Reporting Services. The administrator could then grant read-only access to the end-user to view these reports. Furthermore, the administrator could also export data from the system in different file formats.

The EAU system was developed by a local supplier who is also responsible for its support and maintenance. The NAO observed that the initial contract, which was recently signed between the local supplier and MEDE, has a sound Incident and Change Management procedure[5] in place. The supplier maintains and accesses the system remotely through VPN (Virtual Private Network) using an RSA[6] Token on both the Test Database and the Application Server. The EAU system is still undergoing particular developments and enhancements whereby all software fixes are implemented on the testing environment first before deploying them on the live environment. All these

[5] Refer to Section 5.2 – IT Service Management
[6] Reference: http://www.emc.com/security/rsa-securid.htm

fixes are recorded according to the Change Management procedures. The testing environment is also being used for training purposes especially when an enhancement has been made to the system.

The EAU system is running on a virtualised environment hosted at MITA-01 Data Centre in St. Venera. MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is regularly backed up.

## 3.2 Oliver Library Management system (LMS)

The Schools Library Service (SLS) forms part of the Student Services Department within the DES. The Mission statement is to provide *'Adequate libraries for schools at all levels with appropriate premises, furniture, equipment, book stock and staffing to support the curriculum and literacy incentives'*. Among its services, the SLS:

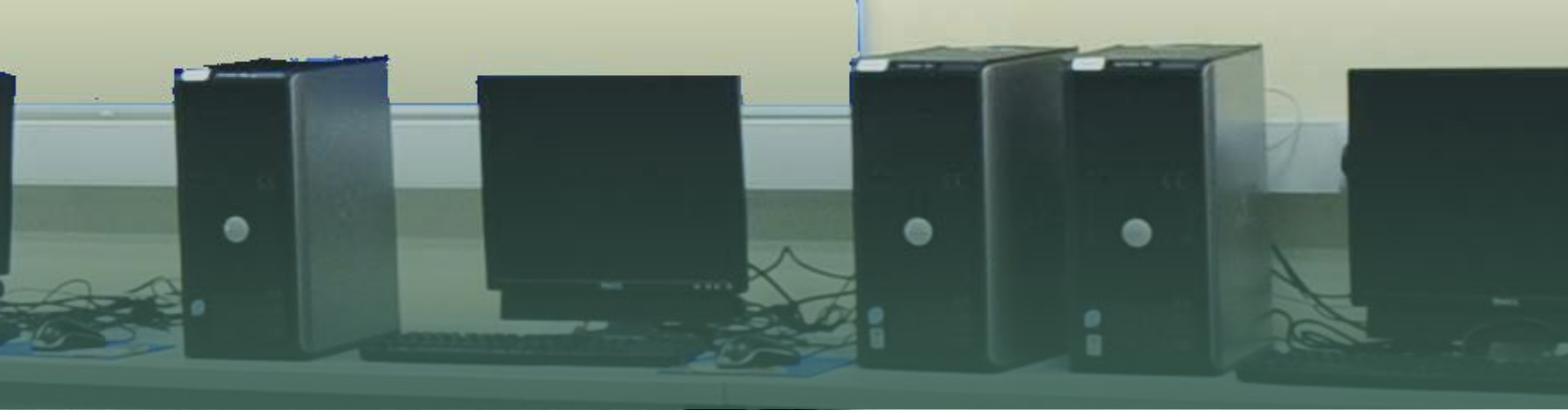
- 'Assists with the introduction of information and communications technology in school libraries especially through the use of computer hardware and software.'
- 'Provides a common database of library materials held in state schools and offers the possibility for non-state schools to join in.'

In 2005, the computerization of school libraries commenced with a pilot project in six different sites. To date, the number of sites has risen to 28 sites, which include 23 State Primary and Secondary schools, two Church Primary and Secondary schools and three Special libraries. The latter are mainly used by the Student Services Department, the SLS and the Specific Learning Difficulties Unit.

Oliver LMS is an off-the-shelf web-based application with a Microsoft SQL database back-end. It has a customisable web page whereby every school library is linked to the main web page, namely http://www.sls.gov.mt. The school librarian can create and update the information without needing any technical knowledge. In this regard, every school librarian can promote new resources, curriculum materials, services or school library events.

The system is designed to record and control resources in both Primary and Secondary schools. It is equipped with a search and display facility for students and staff. Search results are presented and can be obtained through searches, predictive text searching or picture based icons, to assist those students who may not be fully literate.

Through the OPAC (Online Public Access Catalogue), the Oliver LMS provides the students and school staff with the facility to manage and customize their own library profile, add book reviews, reserve, renew items, view their loan information, e-mail



library staff, save, e-mail and print the search results, set up alerts for specific interests. The system notifies students by e-mail of any new material related to their interest that has been added to the central database. Library staff are able to compile reading lists to assist students in their projects. Useful websites can be added and accessed directly through Oliver LMS. Olly is another OPAC interface specially designed for Primary school students.

The SLS manages the Oliver LMS. Whilst all teacher-librarians' user accounts are managed by the SLS, user accounts for students and school staff are managed by their respective teacher-librarian(s). All users are provided with a login and a password. The latter must be changed upon first logon, whereby the new password must follow the password complexity rule, which include a mix of letters and numbers. The NAO observed that passwords do not expire over a number of days and the system will not block access after a series of unsuccessful logon attempts. If the system is left idle, the session is timed-out and the user must login again to the system. Even though the PC is locked, if it is left idle for more than ten minutes, the NAO recommends that the teacher librarian locks the PC if he/she needs to move away from the desk.

To-date, there are 53 teacher-librarians from State and non-State schools, 13 library staff from the SLS, the Special Learning Difficulties Unit and the Students Services Department, who have managerial accounts to access the Oliver LMS.

Following the above recommendation, the NAO were informed that the SLS took immediate action and an internal memo was sent to all school librarians and library staff to lock the PC immediately, if the PC is to be left unattended, thus preventing any misuse of the PC in obtaining unauthorised access to data.

If a user has forgotten his/her password, one can retrieve the password by clicking on the '*Forgotten Password*' link at the login stage. After clicking the '*Forgotten Password*' link, the user is required to enter his/her login and click on the e-mail button. The system checks whether the login is valid before sending the password to the respective user e-mail address. The NAO recommends that since the user's password is sent in clear text via e-mail, a new password should be randomly generated from the system whenever the 'Forgotten Password' is selected. The new password must then be changed upon first logon.

Whenever a user retires or no longer requires access to the system, the Human Resources Department within the DES will inform the system administrator within the SLS to delete the account. On the other hand, all accounts of users who are on prolonged leave, career break or maternity leave are downgraded to the 'default' user level role. In this regard, the NAO observed that the Oliver LMS has different user levels, namely:

- System Administrator – This user level has full access rights to administer the Oliver LMS.

- SLS Staff – All users within the SLS are assigned this role whereby they have full access to the Cataloguing, Circulation and the Online Public Access Catalogue (OPAC).

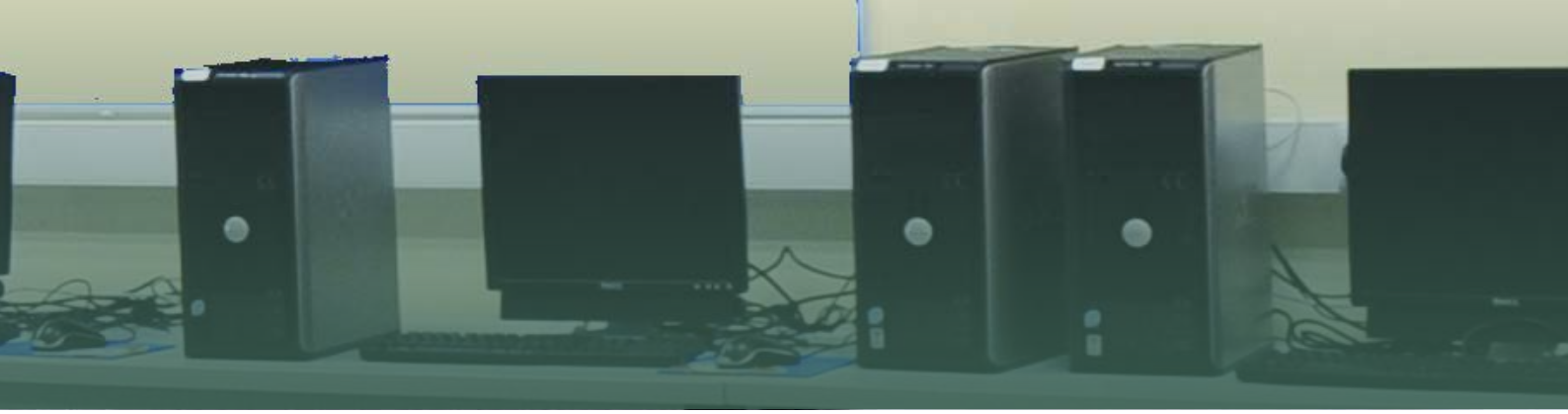
- School Librarians – The SLS system administrator assigns this user role to teacher-librarians who are normally appointed by their respective Human Resources Department. Teacher-librarians have full access to the Circulation and OPAC modules and they can view full bibliographic details, from the Cataloguing module. All School librarians are required to sign a document entitled *'Oliver Library Management System: Terms and Conditions for use by Library Staff'* whereby every school librarian must abide to a set of rules on the proper use of the system.

- Default – Teacher-librarians assign this user role to all teaching staff and students who register as members of their respective school library. This user role permits registered borrowers to have access to the OPAC module, which provides a variety of functions.

- Library Helpers – This user role is assigned to a number of students, within the State Secondary schools, who volunteer to help the teacher-librarians during the mid-day breaks. The library helpers have access to the OPAC module and to the Circulation Desk. However, this does not mean that they can view, edit or add the borrowers' personal data. The Circulation Desk is restricted only to the lending and returning of library materials.

The students' accounts are managed by the teacher-librarians. At the beginning of each scholastic year, the students' personal data, which is available on the Student Teachers' System (STS) database, is uploaded into the system. Teacher-librarians need to assign a username, add the e-mail account, when available, and set the expiry date. On the other hand, teacher-librarians have to create new accounts for the teaching staff.

During the course of this audit report, the NAO observed that even though the system has audit trails in place, these are not accessible by the system administrator. If the latter wishes to gain access to the audit trails, the system administrator has to ask the third-party supplier to provide the necessary report. In this regard, the NAO were informed that the audit trails are now accessible by the system administrator after a new version release was installed in the end of 2012.



The Oliver LMS has different operational modules, namely Cataloguing, Circulation, OPAC and OLLY (a unique OPAC portal for young patrons and students). These are only accessible according to the user levels assigned by the SLS system administrator.

The core facility of Oliver LMS is the central catalogue. The Cataloguing module enables the SLS staff to add bibliographic details of book, and other non-book materials, such as digital versatile discs (DVDs), websites, computer files, games and many more to the central database.

The Cataloguing process is a very time consuming task. The SLS staff, who have been granted access to this module can create or edit templates by adding, removing or updating fields such as the title, subject, author, series publisher, date of publication, collation, notes and many more. The Cataloguing process is done centrally at the SLS, whereby all the library materials are classified according to the Dewey Decimal Classification[7] scheme. The SLS classifies every school's library resources in different collections: Information books, Audio-Visual materials and Project materials are classified under the General collection, Teachers' Resources, Equipment, Readers' sets and Library Science are classified under Teachers collections and Junior fiction, Intermediate fiction, Younger Readers, Maltese Junior fiction and Maltese Intermediate fiction are classified under the Fiction collection. The Reference books and the Melitensia Reference are classified under the Reference collection, while the Special Collections scheme and the Reserved books are classified under the Special collection.

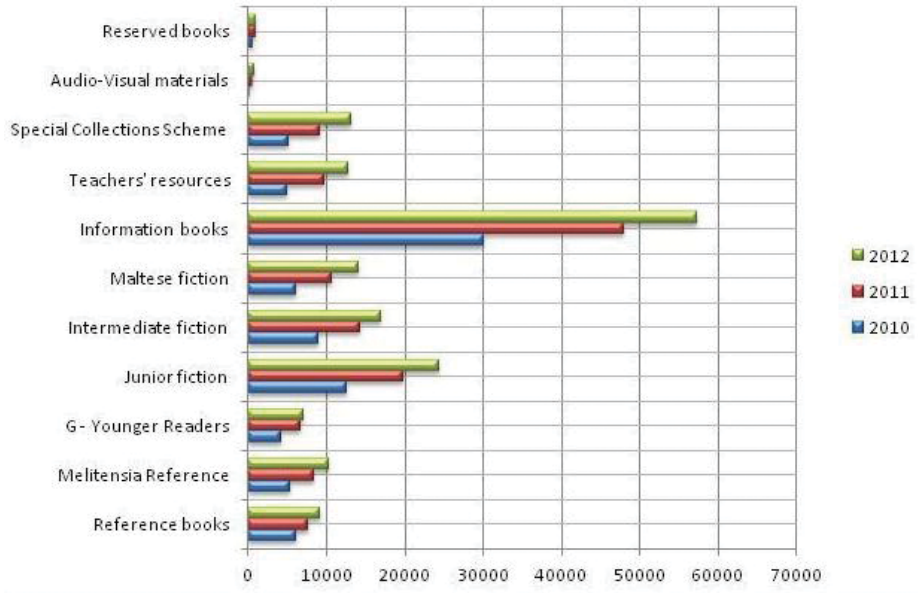



**Figure 5 - Library Resources**

[7] Reference: http://www.oclc.org/dewey/

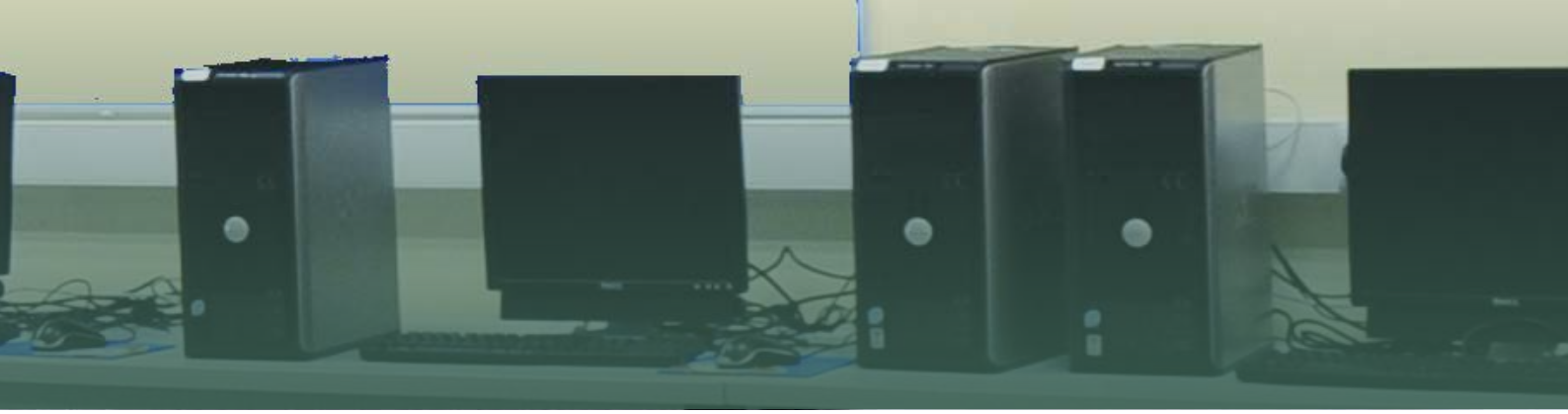
As depicted in Figure four, the NAO is pleased to note that over the past three years, the SLS catalogued library resources falling in the categories shown earlier, whereby the growth is continuously on the increase year after year. At the same time, the SLS removes resources that no longer meet the selection criteria, are appealing and in good physical condition or being used by the students or teachers. This process is called weeding. It is an ongoing process whereby all the material is grouped centrally and removed from circulation. A copy from every item is kept at SLS and stored in the Special Collections Scheme database. The rest is disposed of for recycling purposes. There are definite advantages to regularly weeding the schools' library collection. The main advantage is that every school library will look attractive and inviting to all students and teachers in having a reliable and up-to-date collection.

The Circulation module is used to process loans, returns, reservation and bookings. The SLS created workflows and defined a lending rules matrix to establish the loan limit period and the number of resources a borrower will be able to take out at one go. In this scenario, a resource is borrowed for a maximum of 21 days and the borrower must not take more than three resources at a time. Apart from this, the SLS have defined a borrower loan category whereby all borrowers are grouped into four different categories, namely all borrowers under 14 years of age in primary schools; all borrowers under 14 years of age in secondary schools, all borrowers over 14 years of age in secondary schools and teaching staff. The latter can borrow up to 12 teachers' resources with a loan period of one scholastic year.

The NAO observed that whenever a resource is overdue, the system would generate an e-mail to the borrower. If the borrower does not have an e-mail address, the school librarian will have to save the notice in .PDF format file, print and deliver it by hand to the borrower. The notice will list the overdue items, which will include the title or author, class number, barcode number and the due date. If the item is not returned after the third and final notice, the borrower will then have to pay according to the replacement value.

The OPAC module offers the facility whereby users can reserve a particular resource as depicted in Figure 4. If the resource is available, the user will be informed accordingly by e-mail to collect the item within seven days. This functionality is very useful if the item requested is not available or when a borrower would like to book a resource in advance for any forthcoming project or event. Reservations can also be managed by the teacher-librarians via the Circulation Desk interface.

All the actions carried out in the Circulation Desk session could be viewed in the Transaction log. The latter keeps track of all the loans, returns, bookings and reservations of every resource. However, these transaction logs will be cleared, that is, the history of all the transactions is removed when the current Circulation Desk session is closed. On the other hand, the NAO observed that the system keeps track



of all the loans for every individual, which will include the title, barcode number, classification type, due date and the returned date. A report of the borrower's loan history can be produced whereby a document will be created and then saved or printed. Every loan history record is created every time an item is returned via the return tab option. All the records can be purged according to the number of loan history records displayed. During the course of this audit, the SLS provided the NAO with a statistical report of all the resources that were issued out on loan to students or teachers over a three-year period. It is to be noted that the statistical report as depicted in Figure five below, was issued in December and thus the resources issued out on loan covered only the months of January until November 2012.

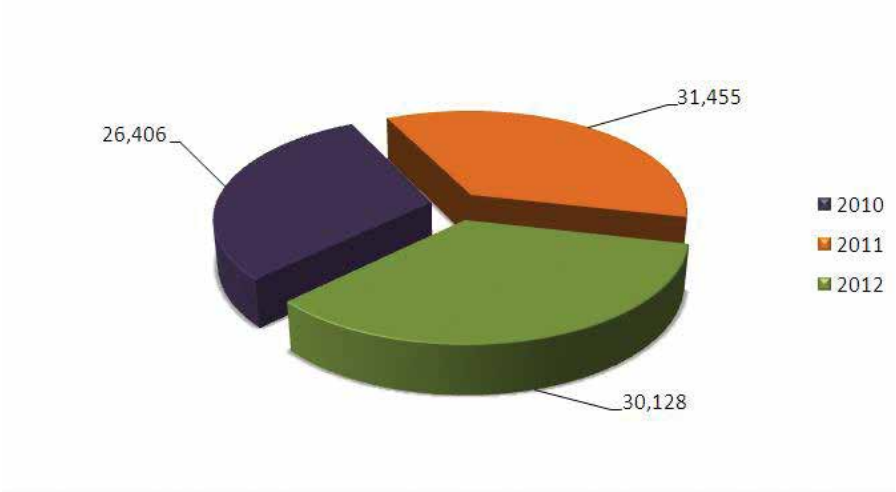



**Figure 6 - Loans Statistics**

The OPAC module is an interactive portal whereby the library borrowers, such as students or teachers, can view their loans, access the catalogue details, retrieve text, images, audio and video files and discover the location and status of physical resources. Users can also place an enquiry or research request, search the content of electronic materials and export and print, e-mail or save search results, whenever and wherever it's convenient for them. Furthermore, users can update their personal details, change password, change their default search type, from basic search to advanced search and change the query operator to find the best match, all the words or any of the words in the query field.

OLLY is an additional OPAC interface that is specially designed for Primary school students and students with mixed abilities. The system has an intuitive interface and offers animated images, fun logos and exciting search techniques with the aim to promote learning and literacy but also makes the library fun and interesting to younger library users.

The Oliver LMS has a search functionality whereby a user can select from a number of options ranging from a basic search to an advanced search using different fields, search by author, subject, series or title. The system makes use of a predictive search or an inflectional search whereby the system tries to match what the user entered with either the word typed or the same word with a different variation.

The NAO observed that whilst the system is being managed by the SLS in terms of account management, the IMU would liaise with the third-party supplier if any maintenance or enhancements were required. In this scenario, the third-party supplier can access the system remotely by means of a secured VPN connection. Any changes applied to the system are recorded through the Change Management process. The latter entails that before any upgrades or modifications are made, the third-party supplier should ensure that the system has been backed up successfully according to the backup schedule. In the event that the previous scheduled backup failed, the third-party supplier can make a temporary backup to disk before proceeding with the change.

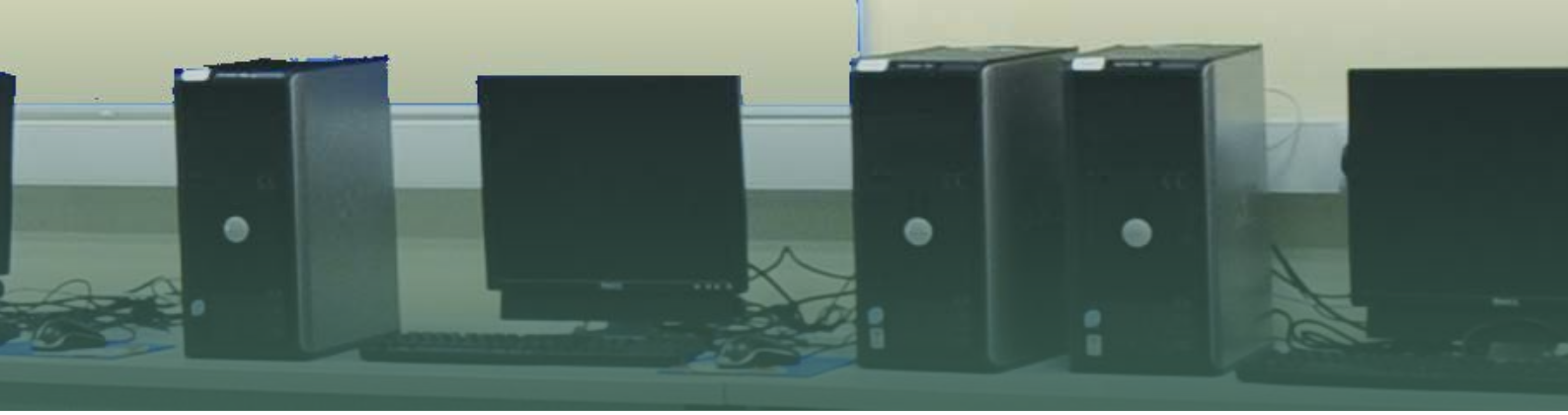
The Oliver LMS is being hosted at MITA-01 Data Centre in St. Venera, which provides a secure access to the server through a VPN connection. Furthermore, MITA monitors and maintains the server in terms of hardware, backups and storage of backup media. The latter are stored in safe repositories at an offsite location.

## 3.3 eLearning Solution

The eLearning Solution is a web-based system, which provides educators with the means to create and maintain their learning materials online and enables the uploading, distribution, grading and storing of students' assignments. This new technology also provides educators with the facility to assess and monitor their learners' progress online and facilitates the transfer of knowledge with other educators in different schools and teaching communities.

Parents on the other hand, can actively participate in their child's learning process and facilitates the means of communication with their children's educators. Thus, the eLearning Solution offers parents with an easy access to their children's learning materials and school work, whilst enabling them to monitor their child's educational progress.

Part of the eLearning Solution consists of a Management Information System where State Colleges keep all the information requested online. This facilitates State Colleges or the Directorates to elicit the information needed. As stated earlier in Chapter 1,



the eLearning Solution is made up of the e1 – Schools Management Information System and the iLearn platform.

The eLearning Solution was implemented in different phases and in 2011/2012 scholastic year, 28 Primary schools within the State Colleges were granted access to e1. All the remaining Primary schools were provided with the eLearning Solution before the 2012/2013 scholastic year.

It is envisaged that by the end of this scholastic year (2012/2013), all the State Colleges in Malta and Gozo will have full access to the eLearning Solution.

Training for school administrators started in January 2012, whilst that for teachers started in February 2012. The eLearning Support teachers were trained in December 2011 and accredited in January 2012, ensuring that the eLearning Centre within the MEDE is fully equipped with the necessary staff that is qualified to deal with the support that teachers in schools might have in using the eLearning Solution.

The local supplier is delivering the initial training of the e1 system to school clerks and the administration personnel. The SIS team is also offering further training to the remaining school clerks and the Schools Management Team (SMT) Every school is provided with a user manual, which was compiled by the SIS Training Centre within the DES. This can also be downloaded from the Skola portal[8].

Teachers were provided training on the iLearn platform by the accredited eLearning Support teachers during the In-Service Training (INSET). Additional notes were also compiled by the eLearning Helpdesk and the Assistant Director for eLearning. These have been uploaded on the Skola portal and on the iLearn's Helpdesk section online.

If further assistance on e1 is required, the clerk can contact the SIS Helpdesk during office hours. On the other hand, if assistance on the iLearn platform is required, the teacher, student or parent can contact the eLearning Helpdesk. The latter offers assistance from 8am till 8pm during the winter period and from 7:30am till 4pm during the summer period.

The e1 system is accessible over the Internet through a secure connection. Every school clerk or teacher is provided with a login, password and a PIN code to access the system. Upon first logon, the end-user must change the password immediately, whereby the password must follow the password complexity rule, which includes a mix of lower case and upper case letters and numbers. Upon successful logon, the system will prompt the end-user to type in part of the user PIN code. The NAO noted

[8] Reference: http://www.skola.edu.mt

that parts of the PIN code requested by the system changes every time a user logs in. If the system is left idle for more than a specified period, the system is logged out automatically. Furthermore, the NAO observed that users could select the *'Remember me'* option in the login page, which will only 'remember' the last previous username. Even though the system has 'two-factor authentication' whereby a user must type in a login, password and PIN code, the NAO recommends that this option be removed to prevent any misuse of the system.

The NAO observed that the system would lock an account for an hour after three unsuccessful login attempts and furthermore, passwords do not expire after a number of days. However, users are advised to change their password regularly, for instance at the beginning of every scholastic term. If a user has forgotten his/her password, the e1 system offers the functionality to click on the "*Forgotten Password*" option. The latter will then generate a new password and sends it to the end user's personal e-mail account. The NAO recommends that passwords expire over a number of days, whereby the user is then prompted to change password upon first logon.

The e1 system is managed by the SIS Training Centre. Whenever a user resigns or retires, the SIS Training Centre is informed and action is taken to de-activate the end user account. On the other hand, if a particular user is on prolonged leave or career break, the system administrator will disable the respective user account. The e1 system has an audit trail whereby it keeps track of user activity and changes into the system.

The NAO observed that the e1 system has different user levels, namely:

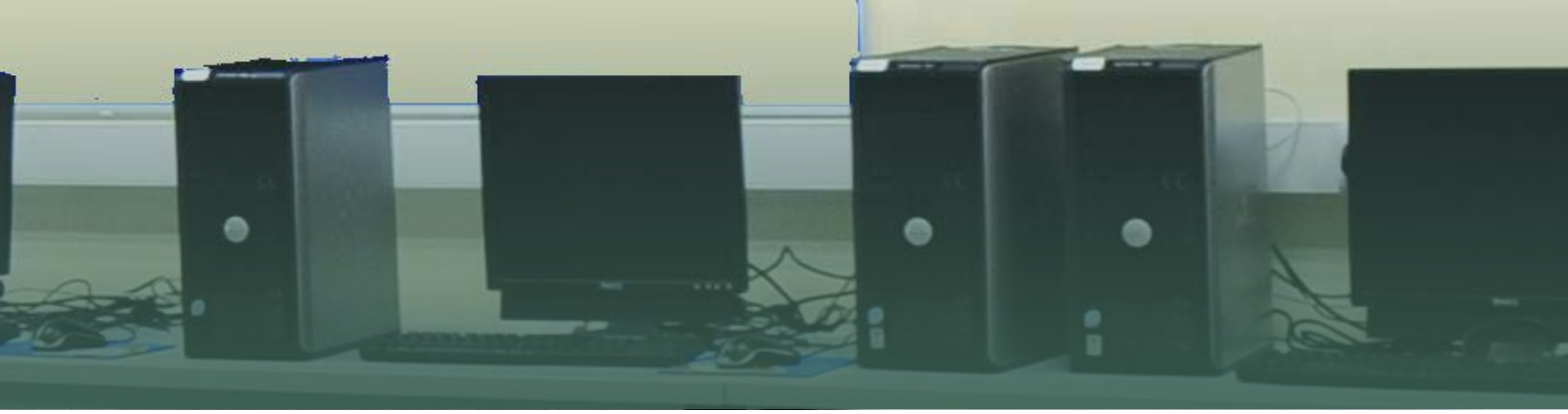
- The *eLC Support* user level has read-only access. It is used within the eLearning Centre, to check basic information of iLearn users when problems arise.

- The *College Principal Office* user level has read-only access. This user level is usually associated with the College Principal and his/her secretary. These users have read-only access to view all the schools' information that fall under the remit of their respective college.

- The *MITA Personnel* user level has read-only access. This user level is associated with the Education Business Cluster[9] within MITA, to be able to view the e1 system.

- The *School Clerks* user level has read, write and modify access rights. It is used by every school clerk to input and modify existing data into the system. However, they do not have any access rights to delete any data from the system. Furthermore, school clerks even have access to the search functionality.

[9] MITA's Organisational Structure: https://www.mita.gov.mt/page.aspx?pageid=194



- The *SIS Support* user level has full access rights. The SIS Training Centre are associated with this user level to manage the e1 system in terms of account management and report functionality.

- The *SMT* user level has read and write access rights. This user level is associated with the Heads and Assistant Heads of Schools. Even though all the schools' information is managed by the school clerk, Heads and Assistant Heads of Schools sometimes access the system to edit any data that is required. Furthermore, the SMT even have access to the search functionality.

- The *Teachers* user level has read and write access rights to the attendance and worksheets only. Every teacher will be associated with this user level to be able to input the examination results in the marksheets that the teacher is assigned to and the class attendance. The teacher can also access other classes in his/her respective school in the event that a particular teacher is replacing another teacher during the day.

When adding a new student, the school clerk inputs the name, surname, date of birth and gender. The system will then check whether the student already exists in the system. If the student information is already in the system, the school clerk has to contact the school where he/she is assigned to transfer the student file to the new school. On the other hand, if no existing record is found, the school clerk can proceed in filling all the student's relevant information, such as ID card number, home address, nationality, details of parents or guardians including name, surname, their respective ID card number, contact number, e-mail address and home address. Once all the data is submitted, the school clerk can then add additional information, for instance if the student requires a LSA, at a later stage.

Apart from the above, the e1 system also caters for the management of personnel within every school. The e1 system handles information of all the teaching staff, supply teachers, administration staff, Heads and Assistant Heads of Schools and records of former staff. The data held includes all contact details, professional qualifications, employment, posts and the information required for statutory returns. The system can link job descriptions with staff, enabling one member of staff to hold multiple posts. It also maintains staff contracts and multiple contracts.

The NAO observed that the system keeps track of all the student history in every school. Thus, if a student is transferred to another Government or Private school, emigrated, expelled, finished Primary or Secondary school or reached school-leaving age, the system will record the school leaving date and the reason behind it. If a student is transferred to another Government school, the receiving school will be informed via e-mail. The school clerk will then check whether the student file already exist in the system before importing the student file and update it accordingly.

The e1 system allows schools to keep track of the students' attendance, by recording and modifying attendance. The latter can also be viewed by individuals or groups of students on a daily or weekly basis, as well as viewing and printing out individual student attendance summary reports and generate alerts regarding their attendance. Heads or Assistant Heads of Schools can identify patterns of absence, continuous and persistent absence and even award students with certificates for high level of attendance. In Primary schools, the student attendance is recorded on the e1 system by the classroom teacher. On the other hand, the student attendance in Secondary schools is recorded differently, since the e1 system is currently being implemented and training is still underway. In this regard, every teacher hands in the student attendance to the school clerk, who will then input all the school attendance manually on the e1 system.

The e1 Reports module is a tool for creating, saving, selecting and printing reports, letters and labels. This feature maintains the consistency of reports, letters and labels generated across the system. Users who have been granted access to the reporting functionality can use the system's pre-defined reports, the user-defined reports, specifically created by the SIS Training Centre, or create reports themselves. Reports created by the users can be printed, exported and saved in Microsoft Office Word, Excel or .PDF format. Other pre-defined reports vary in export options.

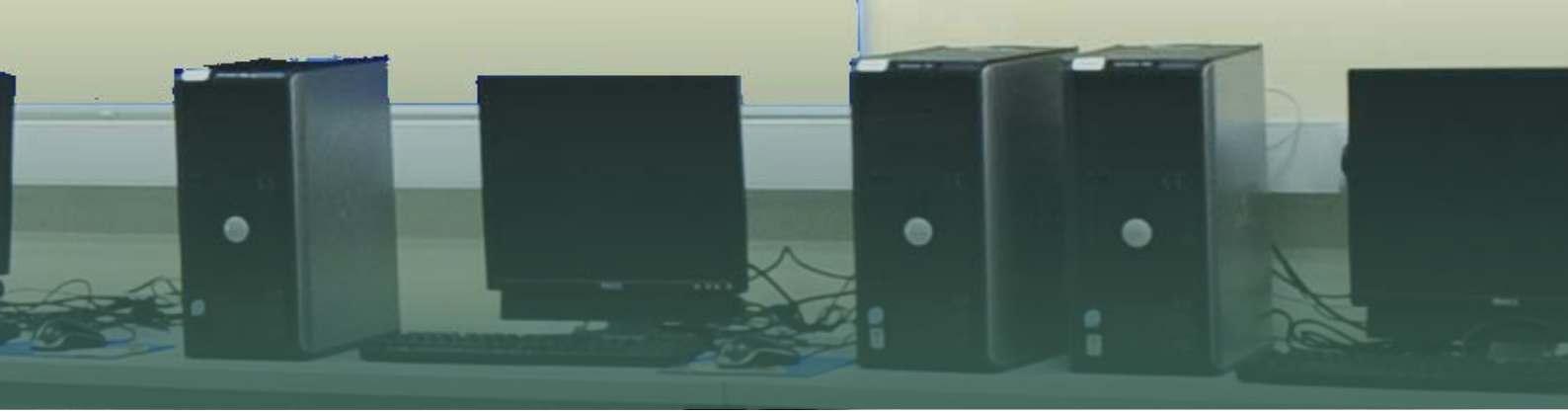
Similar to the previous applications, the NAO observed that the e1 – Schools Management Information system is physically being hosted at MITA-01 Data Centre in St. Venera and managed by the third-party supplier. Apart from the daily monitoring of servers, MITA ensures that the system is backed up regularly, and adheres to Change Management procedures whenever any maintenance is required. The NAO observed that the e1 system has a sound SLA and Business Continuity (BCP) and Disaster Recovery plans (DRP)[10].

## 3.4 TimeTabler system

The TimeTabler was implemented during the summer months and was launched in all Government Secondary schools at the beginning of 2012-2013 scholastic year. It is an off-the-shelf stand-alone application and does not require any login credentials to access it. The TimeTabler is used by every Head of School assisted by the Assistant Heads of School, to schedule the school timetable quickly and accurately.

The TimeTabler is an application whereby the end-user inputs the basic schools' information, the subjects being offered in the school, the duration of every lesson, class names or room numbers, year or form and the teacher's name and initials. The latter are then linked to their teaching subject, class name and year or form. While

[10] Refer to Section 5.4 – Risk Management



data is being populated, the end-user can gain an understanding on the number of teachers linked to a particular subject or the amount of lessons a particular teacher has during the day or week. Once all the data has been inputted into the system, the schools' timetable is scheduled interactively or automatically.

If the timetable is scheduled automatically, the system makes a number of calculations on how to fit a particular lesson or activity. If a problem arises, the system will either switch to interactive mode or else it continues scheduling the timetable automatically. However, this might create problems, as the system does not have the functionality to be able to input operational constraints, which might affect the schools' timetable, example the physical location of classrooms within the school premises.

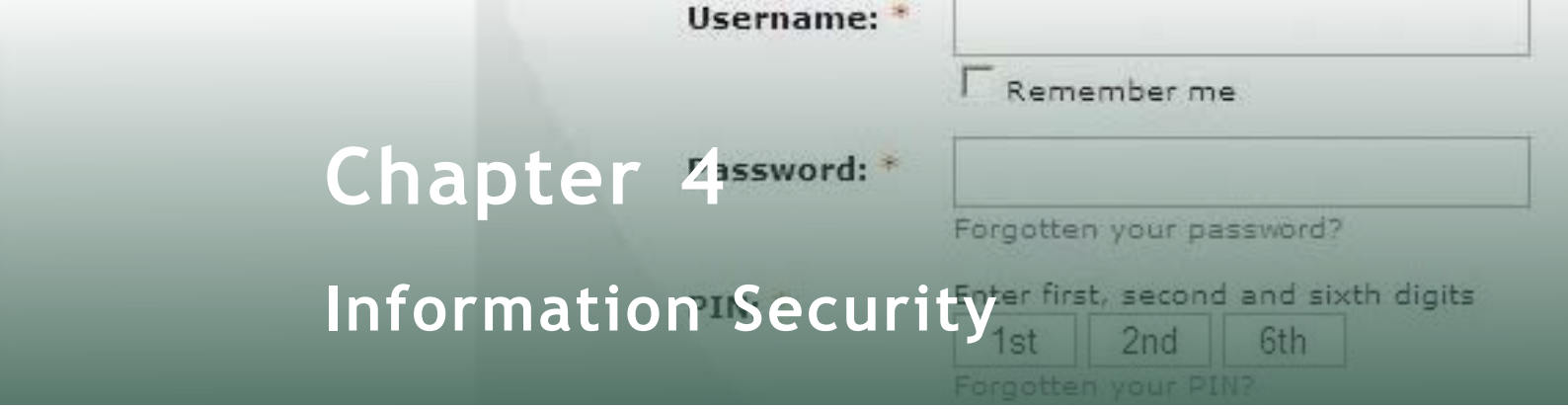
On the other hand, whenever a timetable is scheduled interactively, the system will populate all the data and prioritise which lessons should be fitted first. It also provides the end-user with a number of recommendations where to fit a particular lesson or activity. The end-user can either accept the systems' recommendations or ignore them completely. In this scenario, every Head of School and Assistant Head of School are scheduling their school timetable interactively. Whenever a problem arises, they make careful judgements based on their knowledge and experience before accepting any of the system recommendations.

The TimeTabler offers a number of printing options whereby the Head or Assistant Head of School can print timetables very easily in a number of formats. A timetable can be printed individually for every teacher, subject, class or room. On the other hand, a timetable can be printed in more detail listing all the subjects being delivered by every teacher in each class or room in every day or week. These are normally placed in the administration office or staff rooms for ease of use.

The NAO observed that every timetable could be easily exported and saved in .CSV, .XML, .PDF and other formats. Every school is expected to send their respective timetable to the Education Directorate. Schools will then upload the .XML file in the e1 - Schools Management Information System with the help of the SIS Training Centre.

After the timetable is completed by the SMT member, the timetable is exported from the TimeTabler application and imported to the e1 to create the classrooms and teaching sets, whereby it is integrated with e1 and the iLearn platform. From there on, it can be accessed from any user on the eLearning Solution.

The TimeTabler application also offers a backup functionality whereby the end-user can either backup all the data locally on a PC, where the system is installed, or else on to an external Hard disk, CD or Pen-drive. The Education Directorate informed every Secondary school to backup the system regularly and to store the backup media in a safe place or offsite.




# Chapter 4
# Information Security

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

Information security refers to the processes and methodologies, which are designed and implemented to protect information systems and any confidential, private and sensitive information or data from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption. This might entail amongst others a network disruption as a result of a denial of service (DoS) attempt. Those that result in infections by malicious software, such as malware, will allow a third-party supplier to gather sensitive information or gain unauthorised access to computer systems.

The NAO analysed whether the State Colleges adhere to security policies and procedures to maintain the confidentiality, integrity and availability of data.

## 4.1 Security Management

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

Even though State Colleges do not have or refer to an information classification policy or an information retention and storage policy, they do take precautions on how to prevent the loss of any sensitive information from any of its IT equipment.

### *4.1.1 Disposal of Information*

All State Colleges, in particular the administration office, handle a considerable amount of personal information related to students and academic staff. This information is either stored online on the e1 – Schools Management Information system, locally on a PC or laptop, or printed and kept in a file. The NAO noted that almost every school clerk keeps a hard copy of all the student records in a file. The NAO observed that the administration office ensures that student information is not disclosed outside the school premises. Thus, whenever a file or a particular document needs to be disposed of, the administration office makes use of the shredder machine. The same procedure applies whenever the administration office needs to dispose of data stored on a CD or DVD. The latter is broken, shredded or scored over with a sharp instrument.

As mentioned earlier, all the academic staff within the State Colleges owns a leased PC or laptop. The NAO was informed that all the data residing on the pre-

leasing equipment's Hard Disks is wiped by the third-party supplier as part of the PC Leasing contract. In the meantime, whenever a teacher, resigns, retires or is on maternity leave, he/she must leave the laptop with the Assistant Head in charge of the schools' hardware inventory. The Assistant Head will then fill-in Form B[11] and informs the eLearning Centre accordingly. The NAO noted that sometimes the laptop is immediately passed on to a teacher should there be a pending request for a laptop in the same school. In this regard, the NAO recommends that the laptop is securely wiped and re-imaged with the latest version, before the laptop is handed-in to a different user, to ensure that there is no personal information or any hidden malware residing on the laptop.

In the meantime, the media or documents upon which non-personal information resides are disposed of using the existing recycling or waste disposal process.

### *4.1.2 Backup and Recovery of Data*

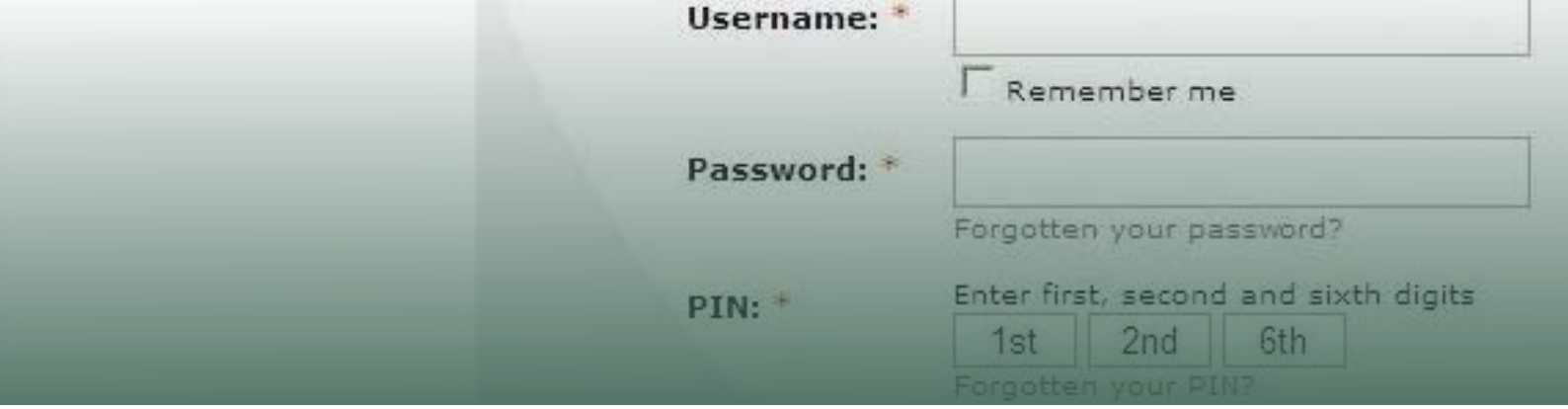
A sound backup and restore plan is critical for reconstructing systems or applications after a disruptive event. The aim of the plan is to recover lost data and to recover computer operations from any loss of data. This might entail a simple restore of lost or corrupted data or a full system restore due to a hardware malfunction or a complete loss of computer operations because of a fire.

The NAO observed that most of the software applications in use in the administration offices or school libraries are backed up online on servers or storage devices. These servers have a backup procedure in place in the form of backup schedules, tape rotations and off-site storage process.

All these servers are hosted at MITA, whose main responsibility, amongst others, is to check and ensure the integrity of the data in accordance with the backup procedures. MITA also diagnoses any issues with such backups as they arise and periodically performs test restores of the backup in order to verify the integrity of the data.

As mentioned earlier, the TimeTabler application, in use within the administration office, is backed up manually. The Assistant Head or Head of School in charge of the TimeTabler application should ensure that the system is backed up regularly to disk and an extra copy of the backup file is stored on a different media, on either a USB memory stick or CD. Even though the system does not contain any confidential information, the media containing the extra copy of the backup file is kept in a secure place in the event that the laptop or the TimeTabler application malfunctions and a restore is required.

[11] Refer to Section 2.6 – IT Inventories




On a similar note, all the teachers should ensure that any data residing on their laptop is backed up regularly either locally on to disk or to an external device, such as a USB memory stick or an external Hard Disk. Even though teachers or administrative staff do not normally store any confidential information, the NAO recommends that the MEDE issues a circular to teachers to raise awareness on the safe use of these external devices, as they can be easily misplaced or stolen if they are not kept in a secure place.

## 4.2 Identity and Access Management

Identity and access management is the process of establishing and proving one's identity and the resources they can access. The aim is to prevent unauthorised access to data, unauthorised use of system functions and programs, unauthorised updates or changes to data, and to detect or prevent unauthorised attempts to access computer resources. In this regard, the NAO observed how State Colleges adopt these processes and what measures are being taken.

### *4.2.1 Authentication*

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

During the course of this audit, the NAO observed that every application that was included in the IT Audit scope, with the exception of the TimeTabler software application, is accessible with a personalised account. Whilst the e1 – Schools Management Information Systems' user accounts are handled by the SIS team, the Oliver LMS user accounts are managed by the SLS. The school clerk or school librarian will liaise with the respective teams mentioned above for the creation, modification, deletion of user accounts. Audit trails are in place to record any changes related to the above user accounts.

The NAO was informed that all the teachers and administrative personnel's e-mail accounts were recently migrated by MITA, to a different Domain. All e-mail accounts are now being managed by the eLearning Centre through the electronic Request for Service (eRFS) form. Whenever an eRFS for the creation, modification or deletion of a user account is raised by the school-authorised person, the CIO will approve the eRFS request. The eLearning Centre will then service the request accordingly.

In the meantime, a similar exercise will be carried out by MITA to migrate the existing Internet accounts to the new Domain. This will facilitate the use of Internet and e-mail accounts through one user account, rather than logging on to e-mail and Internet on to different Domains.


### *4.2.2 Password Management*

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

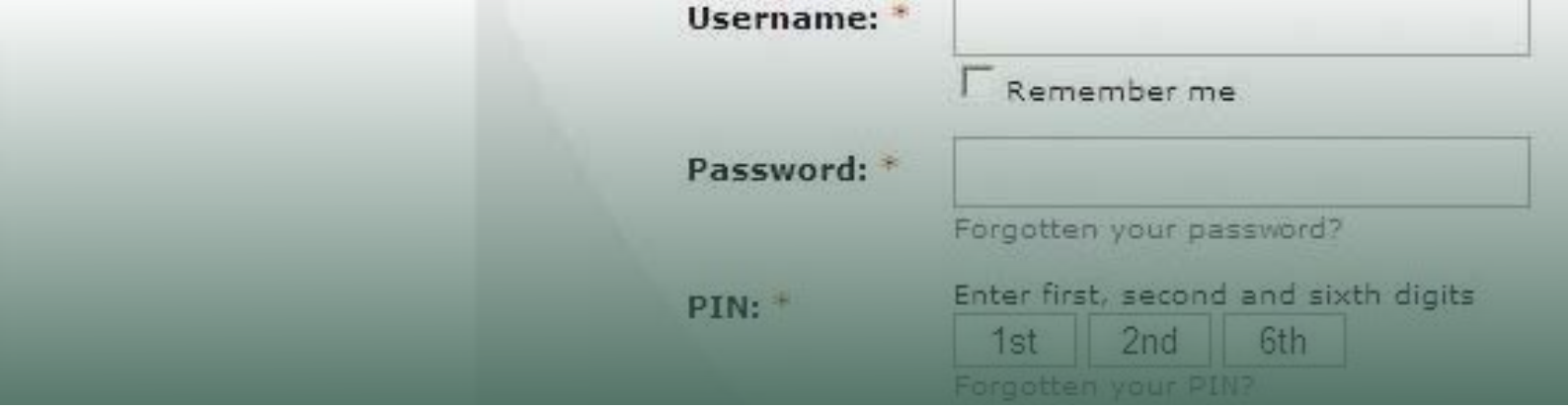
Passwords provide the first line of defence against improper access and compromise of sensitive information.

During the course of this IT audit, the NAO observed that a number of security measures were taken into consideration across a number of applications in use within the State Colleges. The password history settings has been enforced in conjunction with the minimum password age policy setting adopted by MITA, to ensure that old passwords are not continually reused.

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

All account passwords can be easily changed by the user prior to expiration. However, if a user forgets his/her password, the School authorised person is informed accordingly. The latter will then raise the necessary eRFS and a new password is sent to the respective user through the school administration. The user must then change the new password provided upon first logon.

In the meantime, almost every user account password expires over a period number of days. In this regard, the NAO noted that whilst both e-mail and Internet accounts expire after a specified number of days, the e1 – Schools Management Information system user accounts do not expire. To date, school clerks and Head of Schools are requested to change their password regularly, since the password expiry is not enforced. However, even though the passwords can be changed at the user's discretion, most of the passwords tend to remain unchanged. In this regard, the NAO recommends that the password expiry be enforced in the e1 – Schools Management Information System, and should be set similar to the current e-mail and Internet accounts password expiry settings. In the meantime, the NAO were informed that since all student accounts in State Colleges are generic, these have been set not to expire upon MEDE's request. According to the MEDE, it is not feasible to set a password expiry on a generic account, which is used by a number of students.




### *4.2.3 Information Access Control*

Authorised users should not have access to all data and applications and should only have access to those applications necessary to do their particular job. This control also includes data access rights of read-only, read/write or no access where applicable.

During the course of this IT Audit, the NAO observed that all the applications in use by all the administrative staff, school librarians or teachers were granted minimum access rights and privileges required to execute their duties, as per least privilege principle. As mentioned earlier, all requests are handled through the eRFS, which are then approved by the CIO. Once the eRFS is approved, the administrator will then grant access to the user accordingly.

Upon termination of employment, the Human Resources Department within the DES will inform the system administrator to revoke all access rights and to delete the respective user accounts. All these requests are processed through the normal channels, via the eRFS forms. On the other hand, all accounts of users who are on prolonged leave, career break or maternity leave are normally disabled. In the case of the Oliver LMS's user accounts, these are also downgraded with least privileges to the 'default' user level role.

### *4.2.4 Auditing*

Auditing is an important feature in an Identity and Access management process as it provides the necessary trail to explain who, what, when, where and how resources are accessed across the network.

The NAO observed that the audit logs on the systems selected in the audit report are enabled and that access to modify these audit logs is restricted. Whilst reviewing the audit logs, the NAO noted that every system is capable of creating a secure audit record each time a user accesses, creates, updates, archives or deletes information from the system. These audit logs uniquely identifies the user, function performed and the date and time the function was performed.

Since most of the systems are being hosted by MITA, the NAO noted with satisfaction that the Hosting Services Contract Agreement that the MEDE has with MITA, stipulates that all the audit logs are stored in native format and maintained for a period of time, as identified by MITA, to assist in future investigations. As a minimum, database audit logs shall be retained (either online or offline) for the duration of the agreement and the system administrator or third-party supplier shall not delete or modify any of the audit logs prior to relinquishing the Hosting Environment upon expiry or termination of the Hosting Service Contract Agreement. Furthermore, unless it proves that it is not technically feasible, all the logs are retained until MITA specifies otherwise, to meet the data protection requirements.


## 4.3 Security Awareness and Training

Security awareness should be of an ongoing process that seeks to ensure that all users are familiar with the information security policies and best practices that govern the use of IT assets. It is normally disseminated through the normal communication channels either using e-mails, through the publication of leaflets and handbooks or communicated verbally, to ensure that information is conveyed to the appropriate users in a timely manner.

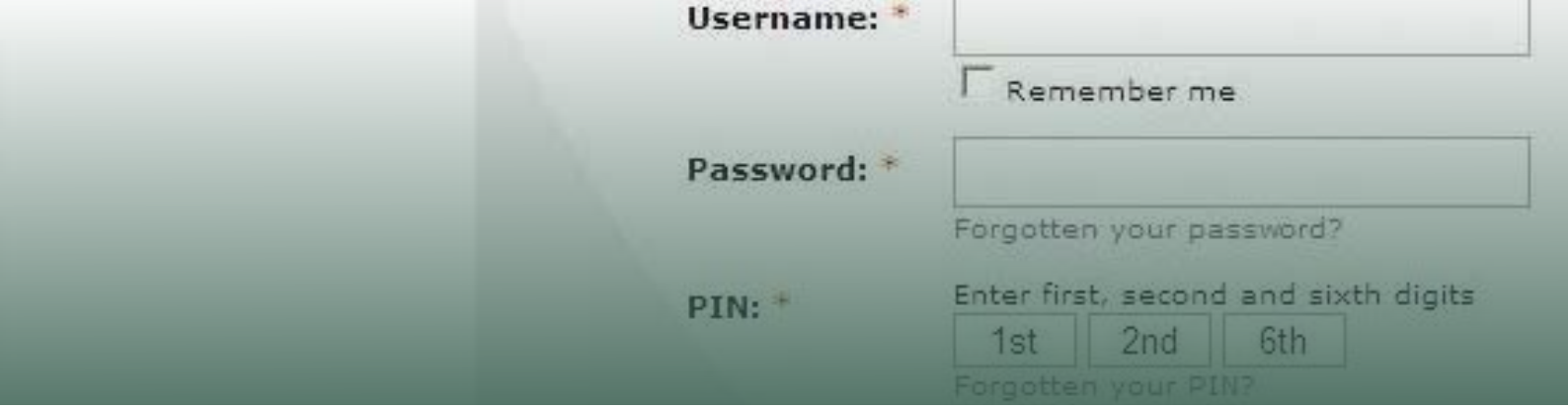
The NAO notes with satisfaction that the DES and the eLearning Centre were involved in the *"BeSmartOnline!"*- a national project aimed at promoting the online safety of Maltese children and youth. The project, a joint initiative between the key local players including the DES, the Foundation for Social Welfare Services, the Malta Communications Authority (MCA), the Cyber Crime Unit within the Malta Police Force and the Office of the Commission for Children, was supported by the Safer Internet Programme of the EU. The EU Safer Internet Programme aims at empowering and protecting children and young people when online, by supporting awareness-raising initiatives and backing the fight against illegal and harmful online content and conduct.

During the 20-month period, which spanned between October 2010 and May 2012, a *BeSmartOnline! Awareness Centre* was set-up to organise various educational seminars and lectures, conferences and information days for children, parents and teachers to raise awareness about the risks associated with Internet use. A number of volunteers were trained to operate a national support line 179 operated by Aġenzija Appoġġ, which is still being offered on a 24/7 basis. Training was also provided to a number of educators and other child centred professionals.

Furthermore, the *"BeSmartOnline!"* portal[12] was officially launched in February 2011. The website contains tips, a link to the reporting mechanism, and other useful links. It also includes downloadable resources for the main target audiences namely children, teens, parents and educators. The development on the site is an ongoing process in order to keep it updated and fresh.

The NAO was informed that the MEDE would be circulating a *"Guidelines for Internet usage in Schools"*, a draft copy of which was forwarded to this office. These guidelines will be in line with and without prejudice to the agreement that was reached in the *"Memorandum of Understanding between the DQSE, DES and the Malta Union of Teachers (MUT) on the Implementation of the eLearning Platform"*. The aim of these guidelines is to ensure that:

[12] http://besmartonline.skola.edu.mt/




- Schools are informed about the applicability of ICT guidelines for Internet usage;
- Users are informed about the security risks of the Internet;
- Internet usage in schools is achieving its' purpose;
- It provides information about teaching the safe and responsible use of the Internet.

These guidelines also explain how the school's network is set up in accordance with best practices, whereby all the websites are being filtered[13] to block websites that are deemed as being unsuitable or undesirable. Teachers are advised to undertake a routine check of sites visited in class and report any concerns to the eLearning Centre. Any misuse of the Internet should be immediately reported to the Head of School and escalated to the eLearning Centre. Finally, these guidelines 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.

## 4.4 Anti-Virus Software

To effectively control and prevent the spread of malware, any department should adopt a reliable Anti-Virus software across its network infrastructure. The NAO observed that in 2012, the eLearning Centre liaised with MITA to replace the existing Symantec Endpoint Protection (SEP) Anti-Virus software installed on all State Colleges leased PCs and laptops with Microsoft Forefront Endpoint Protection.

The Microsoft Forefront Endpoint Protection is built on the Windows 7 Enterprise Operating System and uses the same industry leading anti-malware engine as Microsoft Security Essentials, to protect workstations against the latest viruses, spyware, rootkits and other threats. The engine protects both known and unknown threats, with a combination of highly accurate low false positive rate and behavioural techniques. Furthermore, it ensures that Windows Firewall is active and working properly to protect against network-layer threats.

This Anti-Virus software is updated automatically by MITA through the Microsoft System Centre Operations Manager. The latter provides a single interface for managing and securing all workstations, and implement policies across all State Colleges. Even though MITA is responsible for providing all the necessary support, maintenance and updates related to the Microsoft Forefront Endpoint Protection, the NAO recommends that the eLearning Centre request a periodic report (at least once every scholastic term) from MITA, which computers were infected with malware and if the malware was removed or not. In this scenario, since most of the teachers' laptops are being used at home, the eLearning Centre should continuously educate users and take the necessary measures to prevent similar instances, as this might pose a risk to the network infrastructure within the State Colleges.

[13] Refer to Section 5.4 – Web Filtering

## 4.5 Patch Management

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

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

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

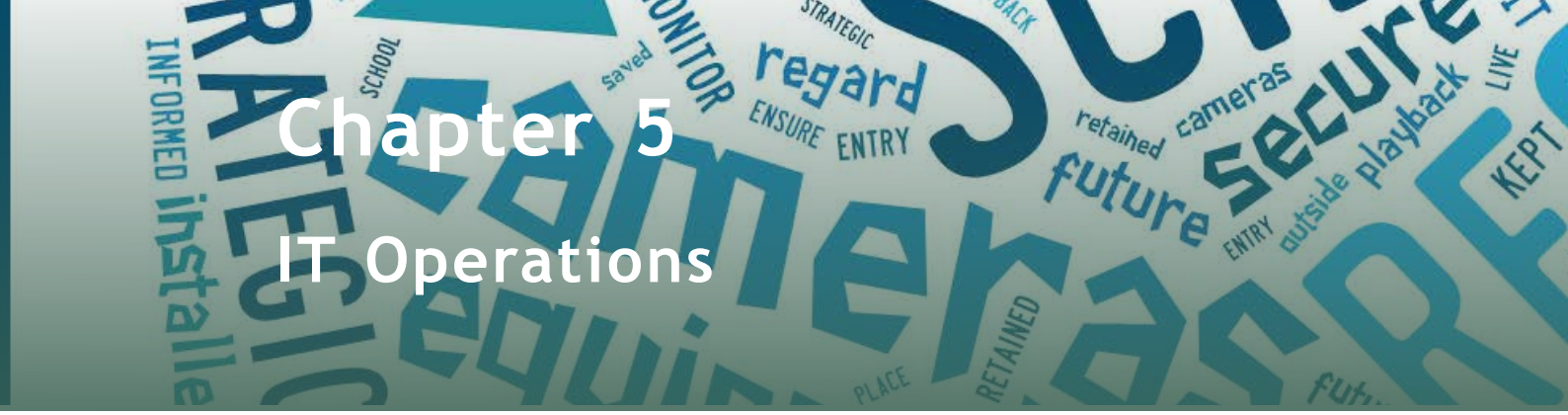
- Hotfixes are used to make repairs to a system during normal operation, even though they might require a reboot. This allows the system to continue normal operation until a permanent repair can be made. Microsoft refers to a bug fix as a hotfix. It involves the replacement of files with an updated version.

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

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

The NAO observed that State Colleges adhere to the standard patch management procedure that is being followed within Government departments. In this scenario, all leased PCs and laptops are configured to automatically download and install product updates through the Windows Server Update Services (WSUS), which is being administered by MITA.

WSUS is a locally managed system that works with the public Microsoft Update website to give system administrators more control, by providing a software update service for Microsoft Windows Operating Systems and other Microsoft Software applications. By using WSUS, MITA manages the distribution of Microsoft hotfixes and patches releases through an automatic update on all leased PCs and laptops in State Colleges.




# Chapter 5
# IT Operations

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

In this regard, the NAO reviewed whether State Colleges are managing and controlling their IT operations in the most effective way to maintain data integrity and to ensure that the IT infrastructure can resist to recover from errors and failures.

## 5.1 Security Controls

During the course of this IT audit, the NAO examined whether physical access and environmental controls are in place to safeguard the number of networking equipment and IT components spread across all Primary and Secondary State schools within the College system.

### *5.1.1 Physical Access Controls*

Physical access controls are designed to protect the computer hardware, software and network equipment from damage, theft and unauthorised access. Therefore, restricting physical access is just as critical as restricting logical access. In this regard, the NAO reviewed the physical access controls that are being adopted in State Colleges.

The Department of School Resources Management is committed to create a secure environment in all schools. A committee was set up to examine the problem and make relevant suggestions to enhance the level of security in schools. A pilot study was carried out in eight schools, in order to draw up a common base line. The department worked in implementing the recommendations in order to ensure a higher level of security in all State schools. A pilot programme for security was conducted in three schools within the St Ignatius College, namely: the Qormi Boys' Secondary school; the Qormi (San Bastjan) Primary school and the Żebbuġ Boys' Secondary school. Three items were introduced: Closed Circuit Television (CCTV), hall-porter and ‘antiporta' with electric lock, while laminated glass was installed on security doors. This programme was extended in almost every Primary and Secondary school within the State Colleges.

Intruder alarms and surveillance systems mitigate the risk of undetected physical intrusion by serving as a detective control as well as a deterrent for would-be intruders. The absence of these controls would increase the risk of theft and other criminal activities. Since all the State Colleges are equipped with leased PCs and laptops, IWBs, projectors and other IT equipment, every classroom or office was equipped with intrusion sensors which were installed in strategic locations within


every room. These are linked to a central control station within the school premises, and only authorised users have access to activate or deactivate the alarm. If the alarm is raised after school hours, the police from the local police station or a private security firm are called in to investigate. Whatever the outcome, the Head of School is then informed accordingly.

Almost all Primary and Secondary schools within the State Colleges are equipped with CCTV cameras to monitor the point of entry and exit in a school. Some schools even have CCTV cameras installed in strategic points outside the school premises and in school corridors within the school. State Colleges must ensure that CCTV recordings are saved and retained for possible future playback. The NAO recommends that the Head of School should ensure that all the saved CCTV recordings are kept in a secure place. In this regard, the NAO were informed that only the Head of School has access to the live and recorded images.

The NAO observed that after school hours, a number of Primary and Secondary schools still make use of the service of a 'watchman'. The role of the 'watchman' is to ensure that windows and main points of entries are locked, and to carry out inspections on a regular basis. However, not all schools have a 'watchman'. The NAO were informed that a few schools even hire third-party security firms who are only called in whenever the intruder alarm goes off after school hours. These firms are being hired by the Head of School and funded by the School funds.

### *5.1.2 Environmental Access Controls*

Environmental exposures should be given the same level of protection as the physical exposures. Environmental exposures are due primarily to naturally occurring events such as lightning, flooding, fire, electrical interruption and other environmental disasters. During the course of this IT Audit, the NAO examined the level of environmental access controls in place within the State Colleges.

The NAO observed that most modern Primary and Secondary schools are being equipped with smoke detectors in strategic locations within the school premises. These are connected and monitored through an alarm control panel, which is the controlling component of a fire or smoke alarm system. The latter are systems, which receive information from environmental sensors, such as smoke detectors, to process the information and then trigger an audible alarm. Whenever the alarm is raised, this can be acknowledged or silenced from the panel. In the event of a power disruption, an alarm can still be triggered as the panel is backed up with batteries. These panels are normally installed in administration offices and only the Head or Assistant Head of School have access to them. However, not all schools have smoke detectors installed within the school premises. In this regard, the NAO suggests that smoke detectors


should be installed, especially in confined zones and areas were the main networking cabinet is installed. Most of the networking cabinets are installed in corridors, administration offices or in the computer labs. However, the NAO observed that in a few cases networking cabinets were installed in a small room, normally used by the school for the storage of boxes or utilised by the school technician. Thus, the NAO suggests that school authorities should remove any items, which might pose a risk to the main networking cabinet, including clutter, storage of files etc, and install a smoke sensor to trigger an audible alarm automatically in the event of a short circuit or fire. Furthermore, the Head of School must ensure that smoke detectors or sensors are regularly tested and certified by a qualified third-party supplier.

As a precautionary measure, all the Primary and Secondary Schools within the State Colleges are equipped with a number of fire extinguishers. These are placed in strategic positions within the school premises and serviced once a year by a third-party supplier. Furthermore, the Health and Safety Officers regularly inspect the fire extinguishers, to ensure that the safety seal is intact and all fire extinguishers have been serviced by the third-party supplier.

Finally, the NAO observed that in the event of a power failure, the main networking equipment and all the leased PCs within the schools' administration offices are equipped with an Uninterrupted Power Supplier (UPS). The latter will safeguard all the equipment connected to them from any power surges or unexpected shutdown.

## 5.2 Health and Safety Unit

The aim of the Health and Safety (H&S) unit within the DES is to provide and maintain a safe and healthy environment in schools by:

- Teaching students about hazards;
- Advising all Heads of Schools against the hazards that were highlighted in the risk assessments;
- Organizing on-going training for school personnel;
- Providing the necessary information, training and supervision required to students and school personnel, to attain the above objectives.

To date, the H&S unit has 16 peripatetic H&S teachers, who are assigned in pairs to cater for all the Primary schools within the State Colleges and the 'special' schools for children with special needs. Furthermore, the H&S unit has 47 H&S teachers who are assigned in Secondary schools within the State Colleges. Overall, this has facilitated the organisation of a structured H&S programme in State Colleges.

The peripatetic H&S teachers emphasise on the upgrading of fire-fighting equipment and fire alarm systems. Every term, evacuation drills are planned and implemented in all State schools in Malta and Gozo. Furthermore, a number of educational programmes


are scheduled during the scholastic year, to raise awareness on health issues, such as basic hygiene (with particular reference to AH1N1) or first aid.

Similiarly, a number of safety audits are carried out in Secondary and Post Secondary schools, during the scholastic year. Apart from the evacuation drills and inspections that are carried out in every scholastic term, the H&S unit organises Safety weeks, which entail a number of seminars and talks by the Malta Red Cross Society on H&S issues.

As mentioned earlier, the H&S unit carries out a Risk Assessment in every school within the State Colleges. The Risk Assessment ensures that every school maintains a healthy and safety environment. Any issues highlighted in the Risk Assessment report, are forwarded to the respective Head of School. The latter must ensure that all the risks identified in the report are seen to, as soon as possible, especially if they pose a threat to an individual. If a student suffers an accident within the school premises, the Head of School must immediately submit a detailed accident report to the H&S unit

## 5.3 IT Service Management

The IT Service Management (ITSM) practices are important to provide assurance to State Colleges and Education authorities that the expected level of service is being delivered.

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

Incident management is reactive and its objective is to respond to and resolve issues as quickly as possible. It is essential for any incident handling process to prioritise items after determining the impact and urgency.

The NAO observed that in every school there is always a person in charge who liaises with MITA, the eLearning Centre or any other third-party supplier whenever a problem with the IWBs, leased PCs and laptops, network, printers or software application arises. In Primary schools, the school clerk is usually assigned to liaise with MITA, the eLearning Centre or any third-party supplier, whilst the Computer Lab technicians or an Assistant Head of School in Secondary schools are usually the ones dealing with any computer related issues and liaising with the respective parties concerned. In this scenario, whenever a call is raised with MITA, a Call Reference Number is generated from their Call Logging system and a notification is automatically sent by e-mail to


the school clerk, Computer Lab technician or Assistant Head of School raising the request. The NAO noted that a number of schools save the e-mail notification either offline or else printed and stored in a file. A few schools even store the third-party supplier job sheet when calling on site and attach it to the e-mail notification.

The NAO observed that most of the schools, which were randomly selected during this IT Audit, are very satisfied with the overall level of support that is being offered by MITA, the eLearning Centre and third-party suppliers. However, most of the schools cannot quantify whether there are any recurring problems on the same hardware equipment or correlate incidents, which are similar in nature, to be able to justify a hardware replacement or solve the root cause of the problem. Thus, the NAO recommends that every school keeps track of all the calls raised in a simple centralised spreadsheet. In this regard, the school clerk, Computer Lab technician or Assistant Head of School can easily trace when a problem was first encountered, whether repetitive calls were made and when the problem was solved.

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

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

Incident management and problem management are related but they have different objectives. Whilst problem management's objective is to reduce the number or severity of incidents, incident management's objective is to return the effected business process back to its *"normal state"* as quickly as possible.

As depicted earlier in Chapter three, third-party suppliers adhere to a sound change management process. This is achieved by formalising and documenting the process of a change request, obtain a written authorisation, carry out the necessary testing, implement the change request and finally communicate to the respective users when the change is completed.

Furthermore, since all the IT applications that were included in this IT Audit report are hosted at MITA-01 Data Centre in St. Venera, whenever MITA requires to carry out a change that may affect the Server where the system is hosted, it notifies all the parties concerned with the plan for the implementation of the change. The latter can be delayed by MITA to allow the third-party supplier to take remedial action as may be necessary, in order to ensure that the proposed changes have no impact on the system. However, the NAO observed that the contract agreement stipulates that MITA reserve the right to proceed with the implementation of the changes, in particular where the changes are deemed by MITA to be of a critical nature.


## 5.4 E-mail and Internet Services

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

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

All State Colleges' Internet services are being provided by MITA through the Government's communications backbone, MAGNET. In this regard, the NAO observed that State Colleges have adopted the *"Electronic Mail and Internet Services Directive"* that was issued by the former Central Information Management Unit (CIMU) in 2003. The NAO noted that this policy has been included in the *"Government of Malta Information and Communication Technology (GMICT) Policy Roadmap 2010-2012"*, whereby this policy is being reviewed by MITA.

The NAO observed that staff were provided with an e-mail account, which was recently migrated to a new directory service (@iLearn.edu), to provide e-mail, web-applications and storage in the Cloud. The NAO was informed by MITA that with the introduction of a new directory service for schools, staff will soon be able to access the Internet through the iLearn account.

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

MITA maintains the right to monitor the volume of Internet and network traffic, together with Internet sites visited. The specific content of any transaction will not be monitored unless there is a suspicion of improper use. In addition, an e-mail sent through the MAGNET that utilises or contains invalid or forged headers, invalid or non-existent domain names or other means of deceptive addressing will be deemed counterfeit. To this effect, any attempt to send or cause such counterfeit e-mail to be sent to or through the MAGNET is unauthorised.

The NAO suggests that the MEDE should periodically notify State Colleges on the relevant points highlighted in the *"Electronic Mail and Internet Services Directive"* especially the restrictions on use of E-mail and Internet services as depicted in Appendix D.


## 5.5 Web Filtering

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

With the introduction of Internet access in all Primary and Secondary schools within the State Colleges, MITA being the Government Internet service provider, has to ensure that the best-in-class web security practices are in place. In this regard, MITA have adopted the *'Web Filtering Directive'* that was issued by the former CIMU in 2003. The NAO noted that this policy has also been included in the *'GMICT Policy Roadmap 2010-2012'*, whereby this policy is being reviewed by MITA. The aim of this directive is to setup methods for controlled access to Internet websites based on Government needs. The directive addresses the legal risk to Government and the productivity of Government Internet account holders.

The web filtering can be configured to either *"whitelist"* or *"blacklist"* a website. Websites found in the *"whitelist"* group can only be accessed when *"whitelist"* is enabled. On the other hand, if *"blacklist"* is enabled, the web filter will allow all websites except those listed in the *"blacklist"*. The NAO observed that even though MITA are providing the Internet service in State Colleges, the web filtering in classrooms and computer labs is being administered by personnel within the eLearning Centre. The web filtering has four different category groups, namely:

- Standard Categories Groups – Websites that fall under this category group can be accessed by students and administrative personnel. This group varies and include amongst others Art/Entertainment, Computers/Internet, Education, Health, News, Sports/Recreation, and Travel related websites.

- Optional Categories – Apart from the Standard Categories Groups, administrative personnel can also be linked to this category group to be able to access Websites related to Abortion, Blogs, Online Storage, Streaming, Web Hosting and Web Applications amongst others.

- All Access – This category is used to list all the groups found in the above categories, which have been granted access to the Internet.

- Banned Categories – All the websites found in this category have been blacklisted and thus cannot be accessed by anyone on the Government network. This category blocks any website related to Adult/Mature Content, Military, Peer-to-Peer (P2P), Remote Access Tools and Weapons amongst others.


The NAO noted that teachers and administrative personnel continuously liaise with the eLearning Centre whenever a website needs to be *"whitelisted"* or *"blacklisted"*. Sometimes, a valid website that falls under one of the above categories is blocked by the web filtering application. In this scenario, the user will inform the eLearning Centre to check the website content, before any changes are applied to the web filtering application.

## 5.6 Risk Management

During the course of this IT Audit, the NAO observed that State Colleges do not have a formally documented business continuity and disaster recovery plan at school level. On the other hand, the State Colleges' IT systems hosted at MITA, including the eLearning Solution, are covered by MITA's BCDR plan. The NAO noted that MITA implemented a number of measures to mitigate the risks involved in the event of a disruption or total failure in the schools' IT systems and network connectivity. Furthermore, all the IT Systems are being backed up daily and all the backup tapes are being stored offsite by MITA.

In this regard, the NAO suggests that the MEDE should perform a Business Impact Analysis and a Risk Assessment exercise in State Colleges from which a BCP and a DRP can be drafted at School level as depicted in Appendix E.

### *5.6.1 Business Impact Analysis*

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

The BIA process is based upon the information that is collected from the College Principals, Head of Schools and key persons within the MEDE. The information can be collected using different approaches. One of the popular approaches is the questionnaire approach whereby a detailed questionnaire is circulated to key users 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 tabulated and analysed for developing a detailed BIA plan and strategy.

In this regard, the NAO recommends that State Colleges lists and reviews its critical and non-critical functions. For each critical function, a State College should then determine:


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

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

After going through this process, State Colleges with the help of MITA or any other third-party suppliers who are providing a service, should determine a recovery strategy to identify the best way to recover a system or critical function in case of interruption, including disaster, and provide guidance based on which detailed recovery procedure is to be adopted.

### *5.6.2 Risk Assessment*

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

Thus, State Colleges should carry out a risk assessment to analyse the value of their assets, identify threats to those assets and evaluate how vulnerable each asset is to those threats. To some extent, a risk assessment is already being implemented by the Health and Safety officers to identify and evaluate the risks that may be caused by natural causes, such as floods, thunderstorms and fire. However, the risk assessment exercise should also include the risks caused by human beings, such as hacking attacks and virus or human errors. A disruption in service caused by system malfunctions, accidental file deletions, network DoS attacks, intrusions and viruses can be classified as a threat to the State Colleges' daily operations. In this regard, a restoration of hardware, software or data files is required to recover operational status and resume service.

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


### *5.6.3 Business Continuity and Disaster Recovery Plans*

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

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

Whilst a BCP refers to the activities required to keep a Primary or Secondary school with the State College running during a period of interruption of normal operation, a DRP deals with the process of rebuilding the operations or infrastructure after the disaster has passed.

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

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

# Chapter 6

# Management Comments

Management concurred with a number of recommendations put forward by the NAO and will be taking the corrective measures to avoid future occurrences. The following comments were also submitted by the MEDE as management comments.

- The Helpdesk and IT Service Management software application needs to cater for the eLearning Solution. A public call for tenders for the procurement of this software is currently being drafted.

- The IPSL personnel continuously liaise with MITA and adhere to a procedure when testing new networking points.

- The MEDE will issue a circular to schools informing them that before procuring any software, a business case must be raised with the IMU. The IMU will then evaluate the impact of such purchase. Schools should also contact the eLearning Centre to test the compatibility of the software procured.

- Another circular should be sent to schools asking for a list of software purchased by the school and used within the school.

- In the case of the eLearning Solution, the first line of support for iLearn is the eLearning Centre, whilst the SIS Team offers first line of support for the e1 – MIS.

- With reference to the password expiry and account lockout rules, one must point out that the Oliver LMS provides such functionality, but it was not deemed feasible, since the majority of users have access to their own details only.

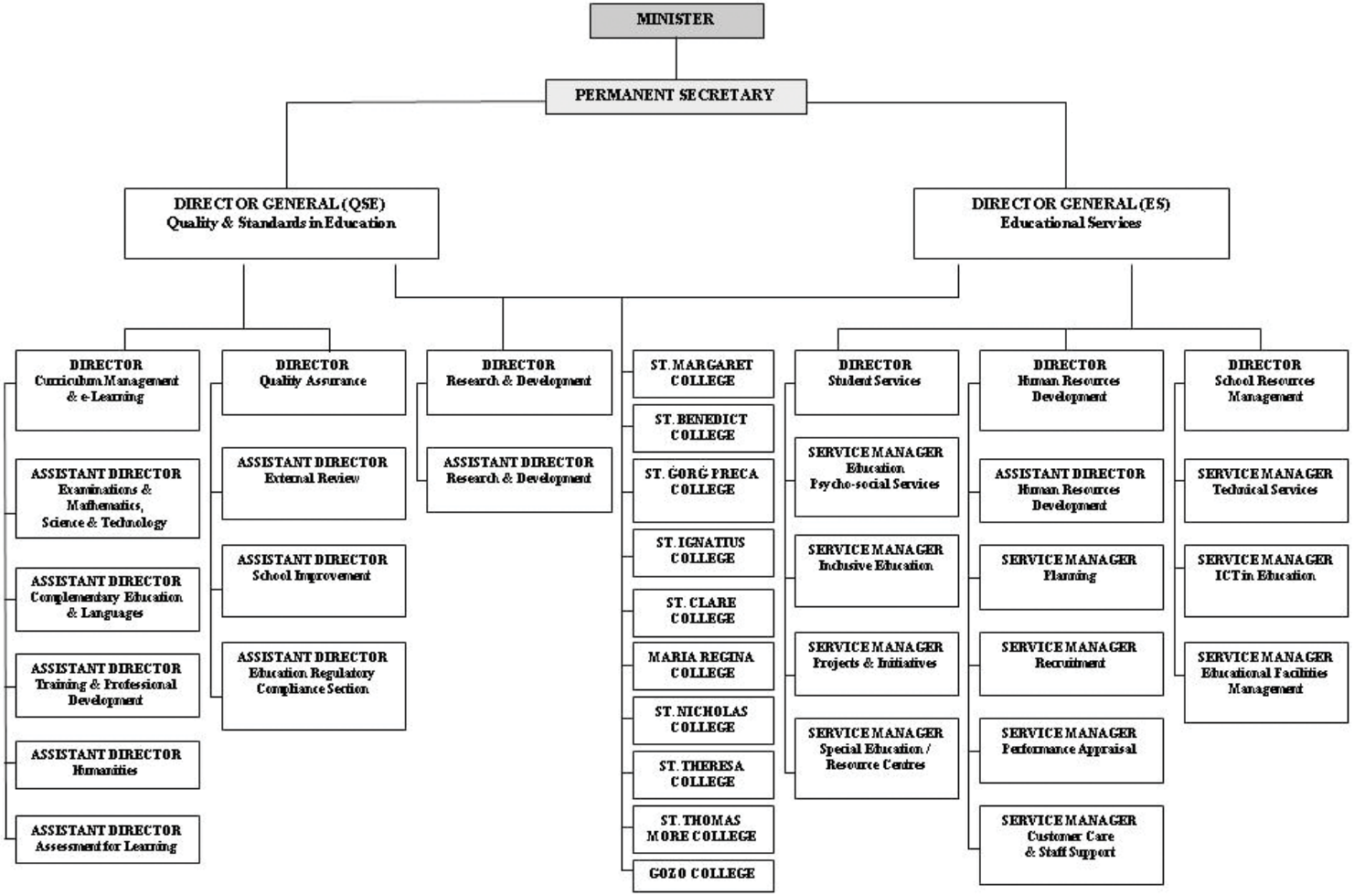
- One must point out that to-date, school textbooks are not included in the Oliver LMS. Even though the system can eventually cater for school textbooks, the responsibility falls under a different department. Furthermore, there are a number of problems that need to be solved, including financial, before this can materialise.

- With reference to the age group in primary schools, the MEDE stated that the SLS followed the contents of legal notice 13/1974, which divides children at age 14. Children attending a primary school are all under 14. Furthermore, using the same Borrower Loan Category facilitates the transition and import procedure, which is done at the beginning of each scholastic year by simplifying matter and keeping the same Borrower Loan Category during the transition.

- e1 keeps track of certain changes affected by the user (e.g. If a student's attendance is changed, an icon appears next to it to notify what the change was and who did the change). When the MEDE was discussing secondary marksheets, they enquired whether there is an audit trail for marksheets. During a meeting arranged by MITA, with the third-party supplier representative, and for which various Assistant Directors and Service Managers related to e1, iLearn and Assessment were present, the third-party supplier representative stated that with respect to marksheets, only an audit that a change has been affected is saved. In such cases, the system keeps track of who performed the change but does not keep a record which field was changed or the original data. In addition, this audit can be made available to the MEDE only upon request and for the marksheets identified by their initial request. The supplier is aware of this, and the MEDE was told in the meeting that this is the only data available in the audit trail.

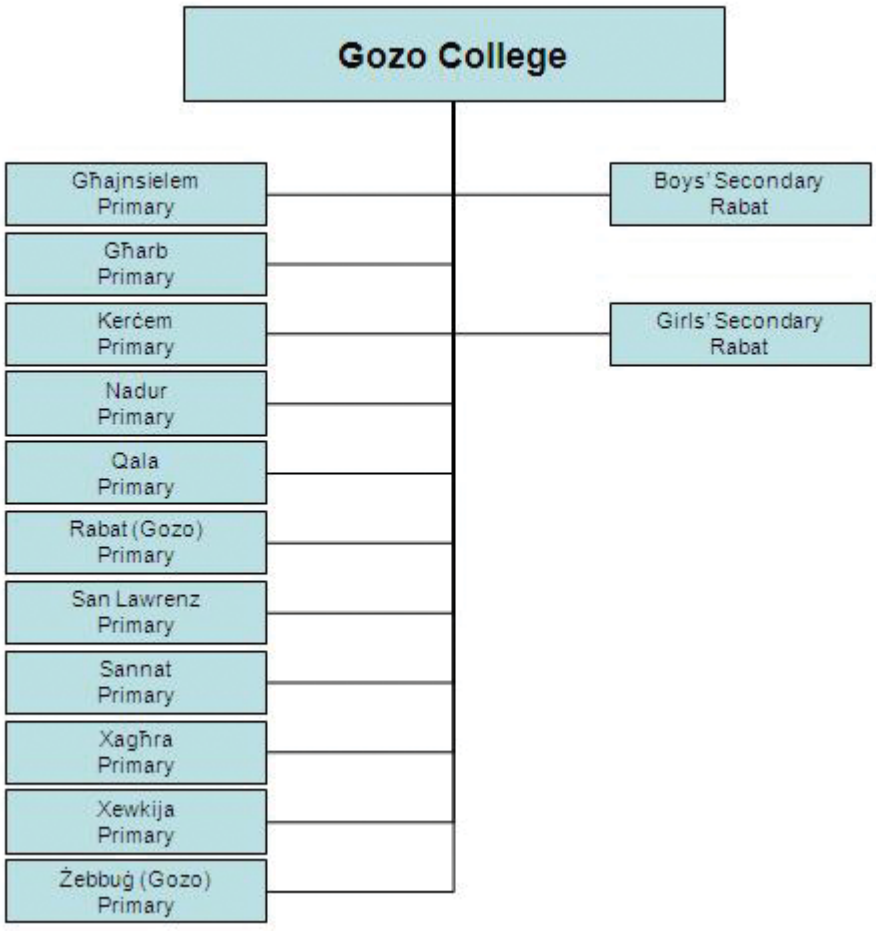
- Although e1 keeps the history record of students, when transferring personnel, all the history is lost. This has been previously pointed out by one of the Service Managers, and the reply given was that e1 is not a Human Resources package. All schools have had the data migrated into e1 according to the STS application, which is being maintained by the Human Resources department. When a new teacher joins a school, his/her basic details are entered by the clerk (something that the clerk and SMT had training for). When a teacher is transferred from a school to another, he/she is linked to the new school in e1 without the need to retype his/her details.

# Appendix A – Organisation Chart[14]




[14] The Organisation Chart in Appendix A was provided by the DQSE within the MEDE

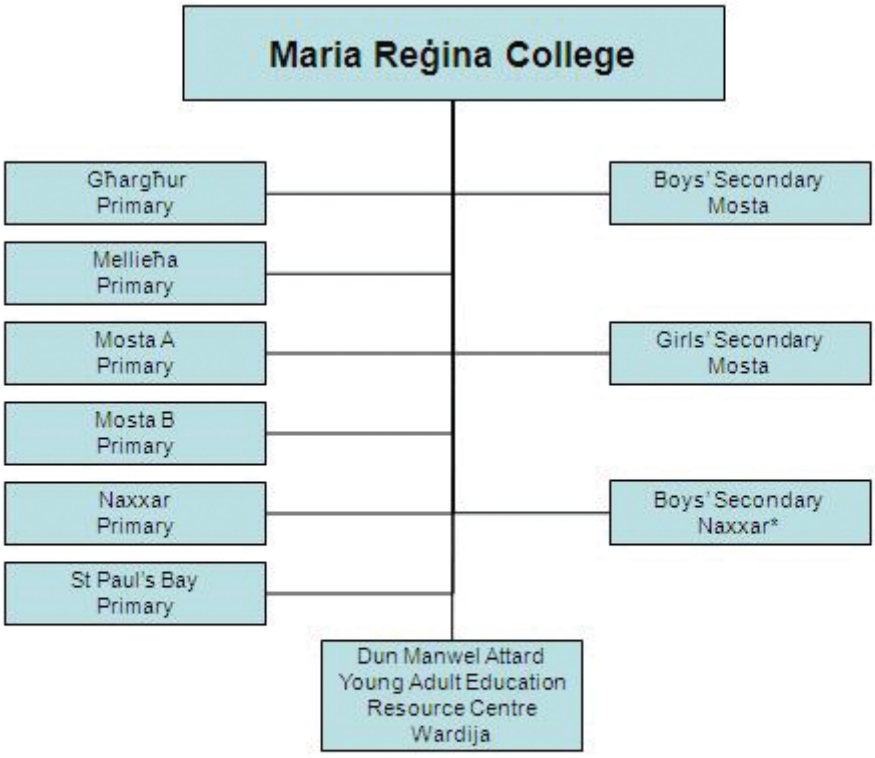
## Appendix B – State Colleges[15]




[15] The Organisational Charts depicted in Appendix B were provided by the DQSE within the MEDE

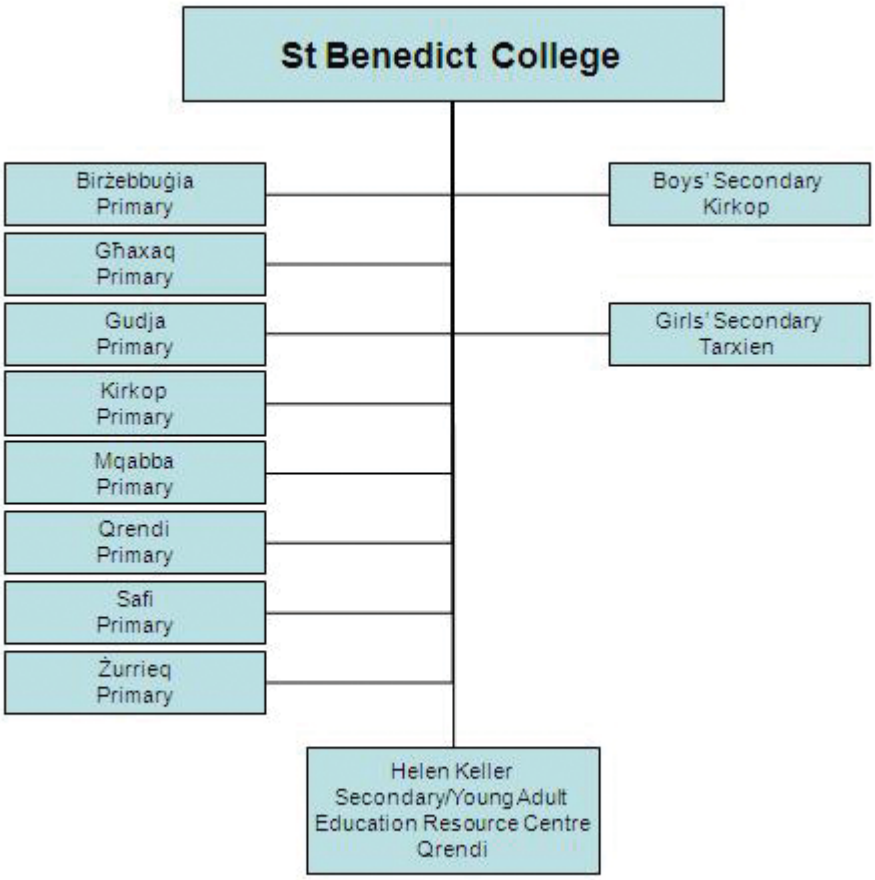
# Appendices

## Appendix B – Cont.



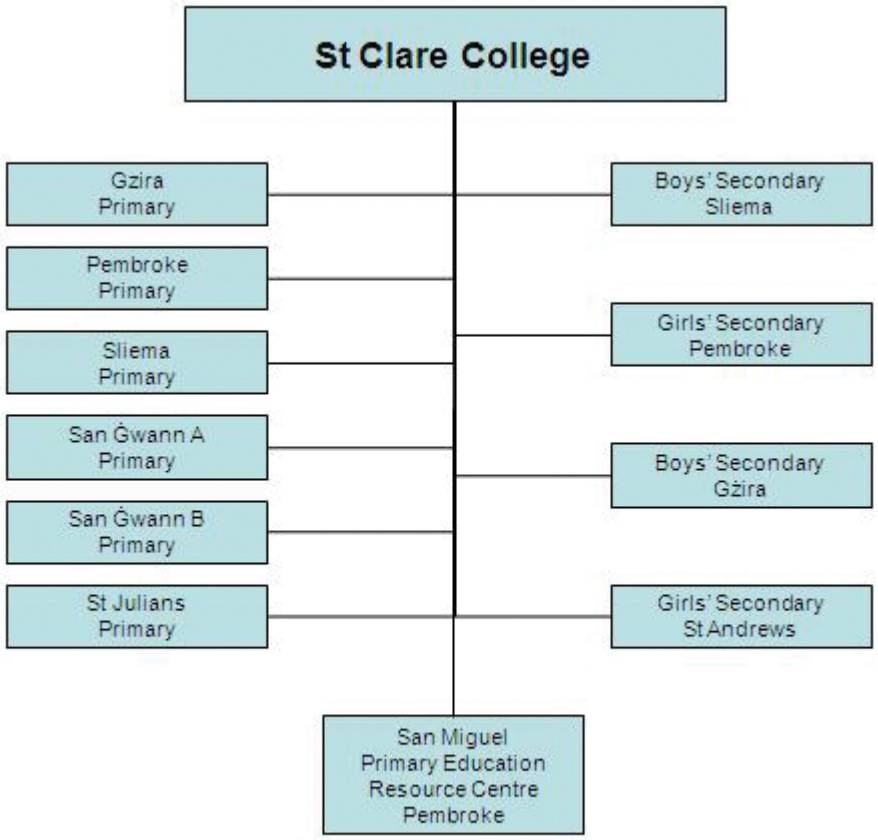

*School Closing down end 2011/12

## Appendix B – Cont.

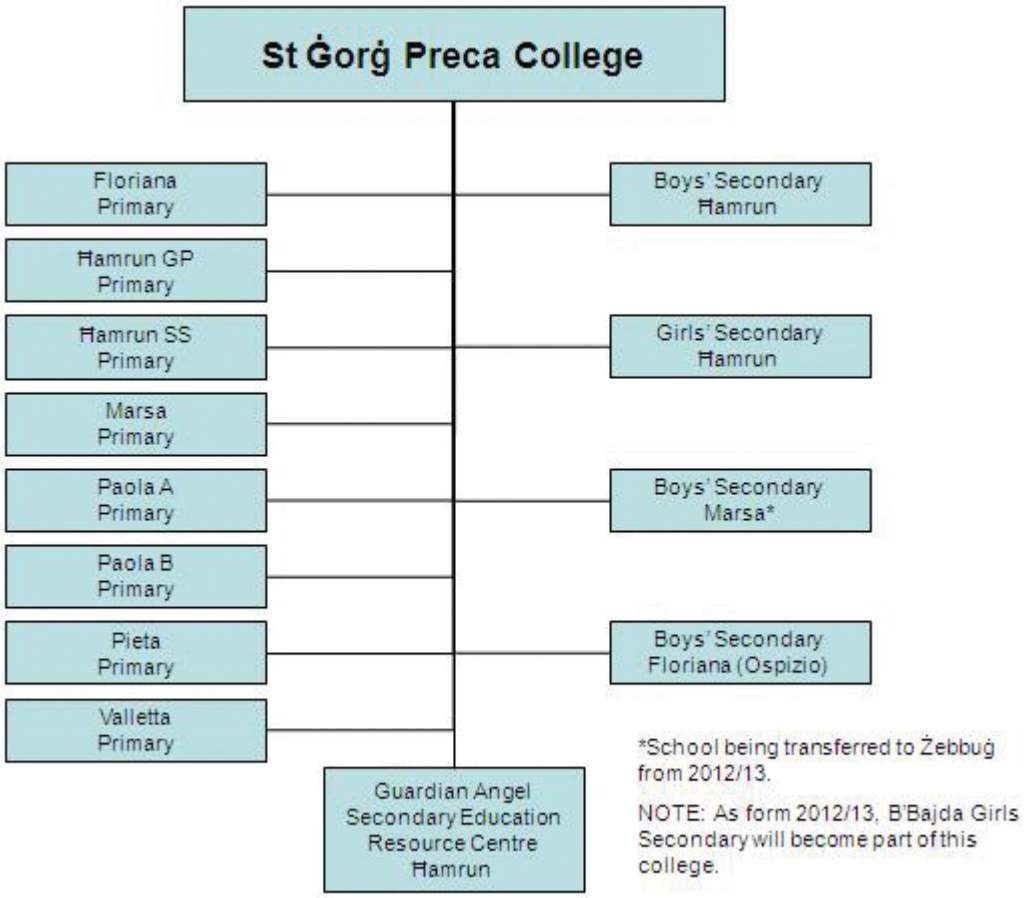


# Appendices

## Appendix B – Cont.

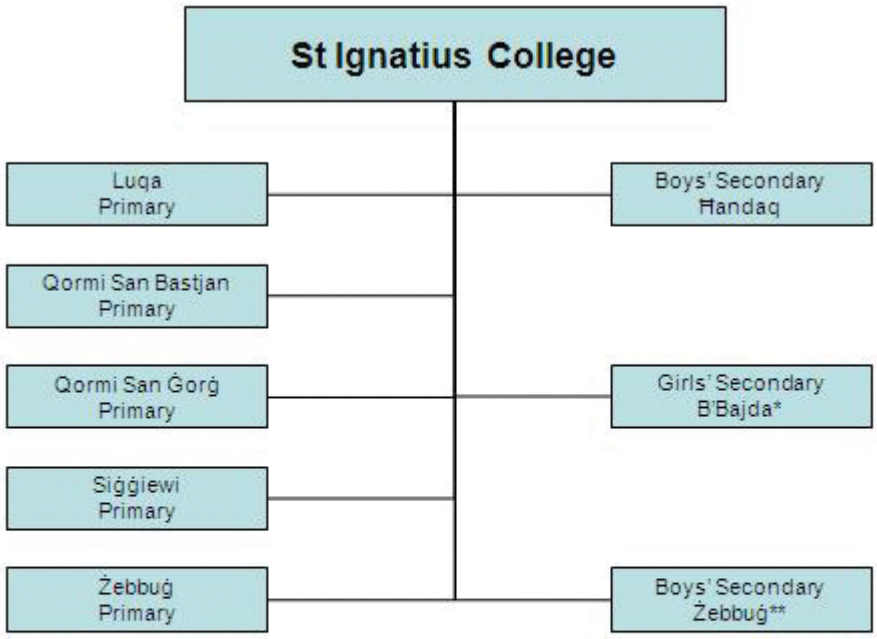


## Appendix B – Cont.



# Appendices

## Appendix B – Cont.

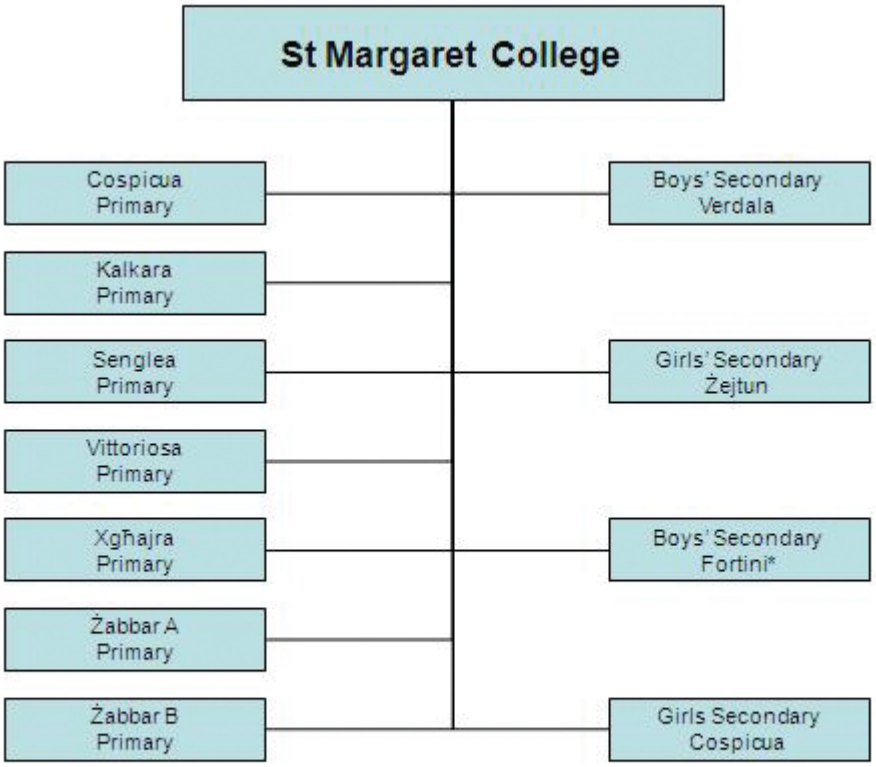



*School will form part of St Ġorġ Preca College as from September 2012

**School closing down at the end of 2011/12

NOTE: As form 2012/13, a new school (Girls' Secondary, Ħandaq) will cater for the girls of this college

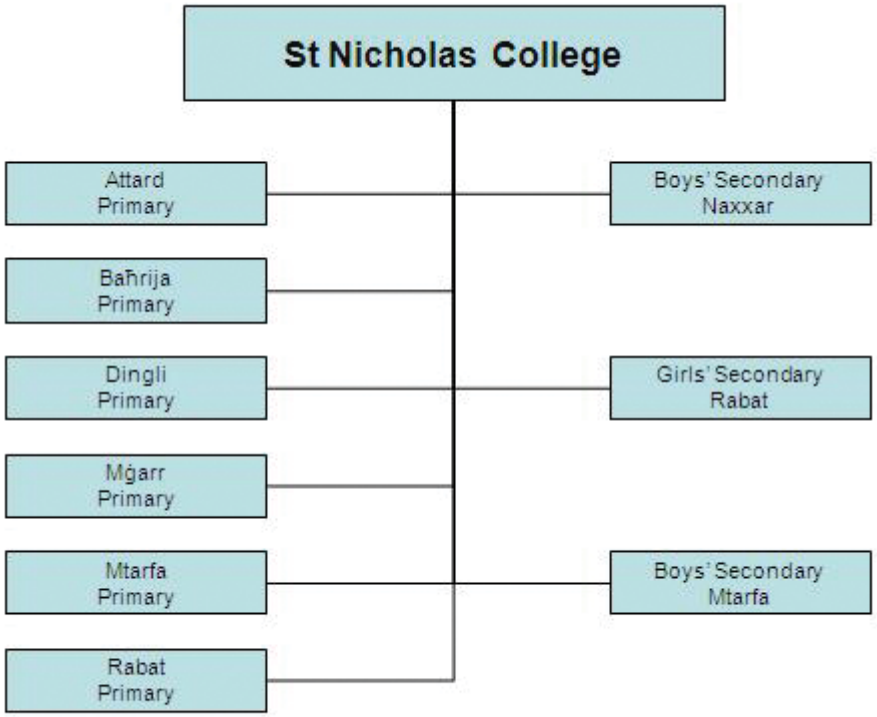
## Appendix B – Cont.



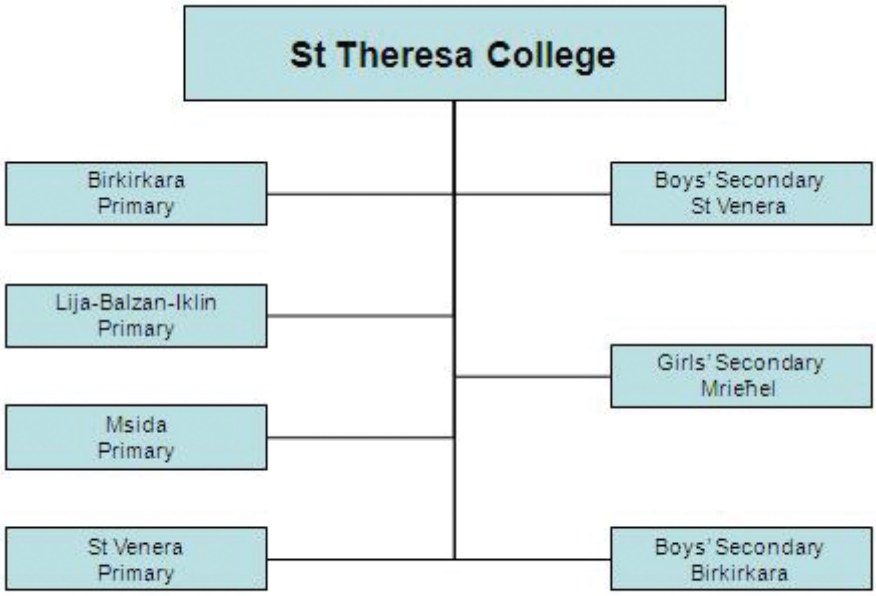

*School Closing down end 2011/12

# Appendices

## Appendix B – Cont.

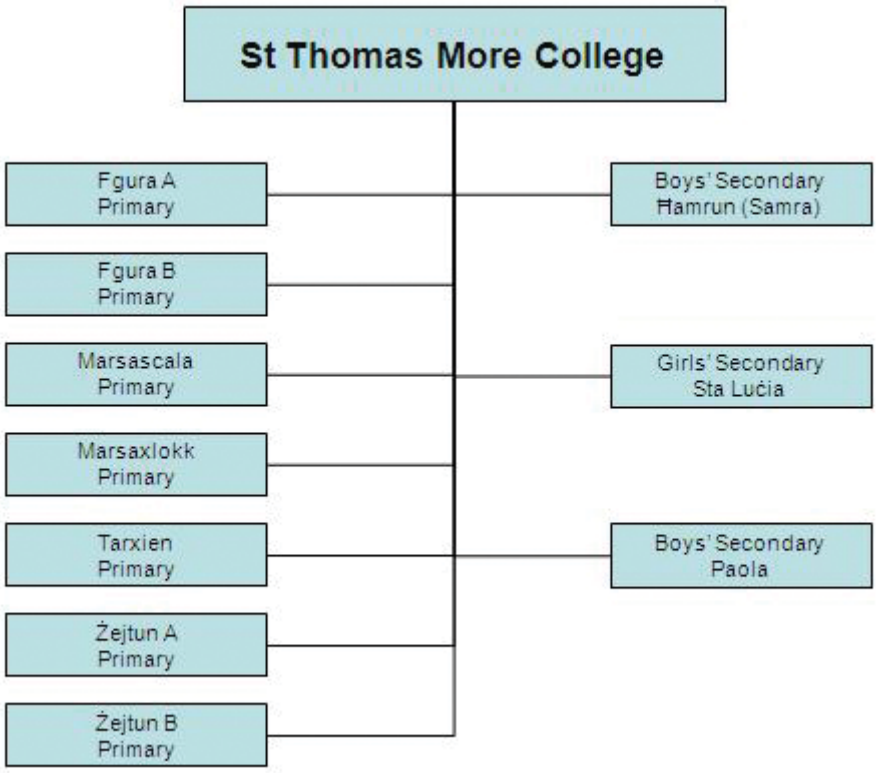


## Appendix B – Cont.



# Appendices

## Appendix B – Cont.



# Appendix C – COBIT Controls

COBIT 4.1 defines IT activities in a generic process model within four domains[16]. These domains are Plan and Organize, 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.

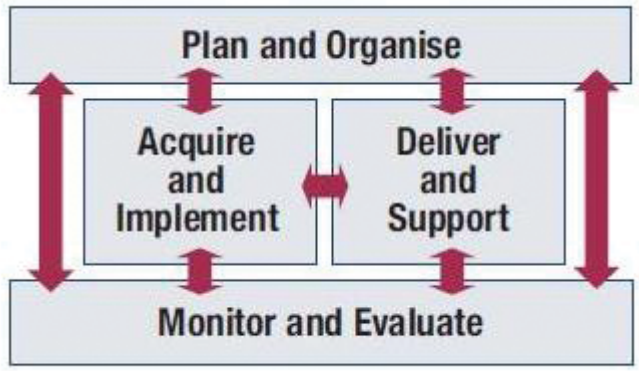



**Figure 7 – COBIT Controls**

## Plan and Organize

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

### *Define a Strategic IT Plan*

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

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

# Appendices

## Appendix C – Cont.

### *Assess and Manage IT Risks*

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

## Acquire and Implement

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

### *Manage Changes*

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

### *Install and Accredit Solutions and Changes*

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

## Appendix C – Cont.

## Deliver and Support

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

### *Define and Manage Service Levels*

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

### *Manage Third-party Services*

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

### *Ensure Continuous Service*

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

### *Ensure Systems Security*

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

# Appendices

## Appendix C – Cont.

### *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.

## Appendix D – Restrictions on use of E-mail and Internet services[17]

### Restrictions on use of E-mail services

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

- Impersonate or forge the signature of any other person when using e-mail.
- Amend messages received in a fraudulent manner.
- Gain access to, examine, copy or delete another person's e-mail without the necessary authorisation from the person concerned.
- Disclose their password or other means of access.
- Use someone else's password or other means of access in a computer.
- Use e-mail to harass or defame any person or group of persons.
- Use e-mail to conduct any personal business or for commercial or promotional purposes.
- Send as messages or attachments items that may be considered offensive, pornography, illegal material, chain letters, or junk mail.
- Send e-mail in bulk unless it is formally solicited.
- Place Government-assigned e-mail address on non-official business cards.
- Send trivial messages or copy messages to people who do not need to see them.
- Send unsolicited mass e-mailing to more than twenty-five (25) e-mail users, if such unsolicited e-mailing provoke complaints from the recipients.
- Use the service of another provider, but channelling activities through a MAGNET account as a re-mailer, or use a MAGNET account as a mail drop for responses.

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

# Appendices

## Appendix D – Cont.

### Restrictions on use of Internet services

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

- Download files from the Internet without adhering to existing policies on virus control.
- Download material (including software) that is not work-related.
- Enter into any contract over the Internet without approval from the appropriate Head of Department or his/her delegate.
- Use the Internet to conduct any personal business or for personal commercial purposes.
- Post a single article or advertisement to more than ten (10) Usenet or other newsgroups, forums, e-mail mailing lists or other similar groups or lists.
- Post to any Usenet or other newsgroup, forum, e-mail mailing list or other similar group or list articles, which are off-topic according to the charter or other owner-published FAQ or description of the group list.

## Appendix E – Business Continuity and Disaster Recovery Plan[18]

A Business Continuity Plan should:

- Be consistent with the schools' overall mission, strategic goals and objectives.
- Be documented and written in simple language and understandable to all.
- Provide management with an understanding on the adverse effects on a particular school, resulting from normal systems or service disruption and the total effort required to develop and maintain an effective BCP.
- Identify the information assets related to core business processes.
- Assess each business process to determine its criticality.
- Validate the RPO and the RTO for various systems and their conformance to the schools' objectives.
- Identify methods to maintain the confidentiality and integrity of data.
- Ensure that an appropriate control environment (such as segregation of duties and control access to data and media) are in place.
- Ensure that data is regularly backed up on storage media.
- Ensure that appropriate backup rotation practice is in place and backups are retrievable.
- Ensure that storage media are kept offsite and kept securely in a backup safe.
- Identify the conditions that will activate the contingency plan.
- Identify which resources will be available in a contingency stage and the order in which they will be recovered.
- Identify the key persons responsible for each function in the plan.
- Identify the methods of communication among the key persons, support staff and employees.

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

# Appendices

## Appendix E - Cont.

- Implement a process for periodic review of the BCP's continuing suitability as well as timely updating of the document, specifically when there are changes in technology and processes, legal or business requirements.
- Develop a comprehensive BCP test approach that includes management, operational and technical testing.
- Implement a process of change management and appropriate version controls to facilitate maintainability.
- Identify mechanisms and decision maker(s) for changing recovery priorities resulting from additional or reduced resources as compared to the original plan.
- Document formal training approaches and raise awareness across State Colleges on the effect this might have on a particular school in the event of a disaster.

A Disaster Recovery Plan should contain the following information:

- A statement detailing the scope and capability of the disaster recovery plan, exactly when should this plan be used and what is the impact on schools.
- A description of the key roles and responsibilities so that anyone assigned to a particular role in the recovery team understand what is required of them.
- A summary of the critical services, their recovery objectives and recovery priorities.
- Third party contact details, particularly those that may be required to assist in the recovery of resources or services that are being maintained within the school.
- Detailed recovery activities and sequence of events, including pre-requisites, dependencies and responsibilities.

## Recent NAO Publications

**NAO Audit Reports**

| | |
|---|---|
| February 2011 | Performance Audit: Renewable Energy in Malta - Follow-up |
| March 2011 | Performance Audit: Road Surface Repairs on the Arterial and Distributor Road Network |
| 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 |

**NAO Work and Activities Report**

| | |
|---|---|
| January 2013 | Work and Activities of the National Audit Office 2012 |