N A O
National Audit Office
MALTA

IT Audit:
Department of Examinations

October 2021

N A O
National Audit Office
MALTA

IT Audit

Department of Examinations

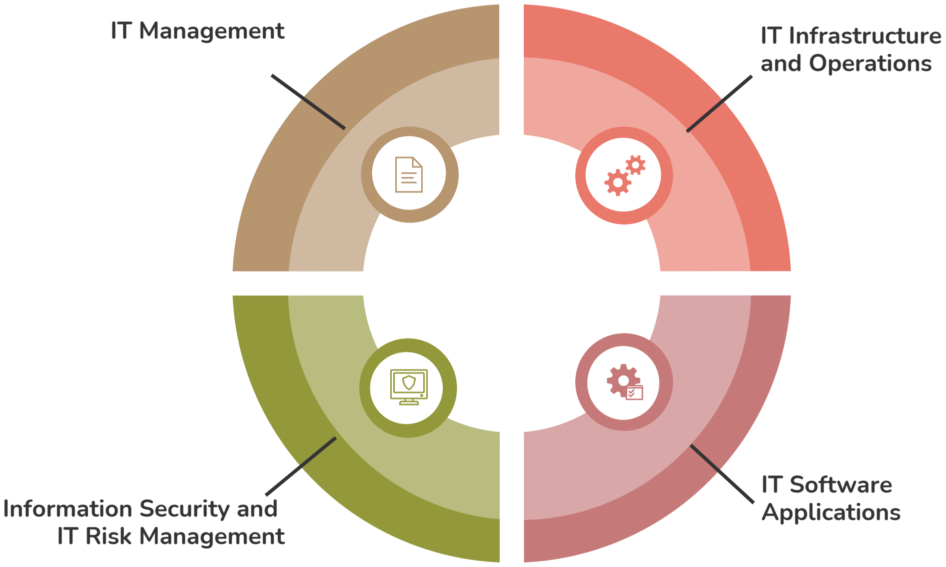
Report by the Auditor General
October 2021

Table of Contents

List of Abbreviations

AQA	Assessment and Qualifications Alliance
BCP	Business Continuity Plan
CCTV	Closed-Circuit Television
CDB	Common Database
CDR	Corporate Data Repository
CFMS	Corporate Financial Management Solution
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
DAS	Departmental Accounting System
DoE	Department of Examinations
DRP	Disaster Recovery Plan
EMS	Examinations Management System
GMICT	Government of Malta ICT
ICT	Information and Communications Technology
IMU	Information Management Unit
ISACA	Information Systems Audit and Control Association
IT	Information Technology
MAGNET	Malta Government Network
MATSEC	Matriculation and Secondary Education Certificate
MEDE	Ministry for Education and Employment
MFED	Ministry for Education
MITA	Malta Information Technology Agency
NAO	National Audit Office
RFS	Request for Service
SSRS	SQL Server Reporting Services
UoL	University of London
URL	Uniform Resource Locator
VMS	Visitors’ Management System
VPN	Virtual Private Network

Key Recommendations


IT Management
IT Infrastructure and Operations
Information Security and IT Risk Management
IT Software Applications

Chapter 2 - IT Management

- Drafting IT strategic plan and annual allocation of IT budget
- Secure wiping of data prior to transfer or disposal of IT equipment
- Read-only access to IT inventories maintained by IMU-MFED
- Recruitment of a full time IT officer

Chapter 3 - IT Infrastructure and Operations

- Adequate location of network cabinet at DoE's new offices with the recommended features and controls
- Revise current backup procedures and issue clearly defined guidelines or policy
- Drafting of SOPs to cover confidential access to audit logs of DoE systems
- Drafting a policy governing the use of personal portable and mobile devices within DoE's offices

Chapter 4 - IT Software Applications

- SLA for the DoE website
- Programming manuals for EMS application
- Discuss with IMU-MFED the existing pool of MFED's education IT systems for possible access
- Further use of social media platforms

Chapter 5 - IT Information Security and IT Risk Management

- Adequate physical access, CCTV, fire prevention and suppression controls at DoE's new premises
- Draft Business Continuity Plan and Disaster Recovery Plan
- Organize regular IT security awareness training sessions for DoE personnel

Executive Summary

The scope of this Information Technology (IT) audit was to analyse the overall IT setup of the Department of Examinations (DoE) focusing mainly on the core IT systems. In this context, this audit sought to determine whether the DoE had the necessary controls in place to maintain the confidentiality, integrity and availability of data, ensure the efficient use of IT resources, as well as to identify any potential risks and make the necessary recommendations to mitigate such risks.

Chapter 2 covers the IT management outlook and reviews the management of Information and Communications Technology (ICT) resources at the DoE. The following are the key findings and recommendations made by the National Audit Office (NAO) in this chapter:

a) NAO noted that the DoE does not have a formal IT strategic plan nor specific annual IT budget, and recommended that such a plan is drafted and budget estimates are discussed with the Ministry's Information Management Unit (IMU).

b) The DoE did not confirm the process adopted for wiping data when transferring or disposing of its IT assets, and the NAO recommended that DoE ascertains that all data residing on such IT equipment is securely wiped prior to transfer or disposal.

c) The NAO noticed that the DoE does not have access to its IT inventories, which are maintained by Ministry for Education's (MFED) IMU, and recommended that read only access of these inventories is provided to DoE.

d) Given the absence of a dedicated IT team/unit at the DoE, and the continued reliance on the support of IMU-MFED and the Malta Information Technology Agency (MITA), the NAO suggests that the DoE management should look into the possibility of engaging a full time IT officer.

Chapter 3 deals with controls concerning the IT infrastructure and IT operations at the DoE. The following are the key findings and recommendations included in this chapter:

a) The NAO recommended that DoE ensures that the network cabinet to be utilised at the DoE's new offices, is installed in a separate room, as well as being adequately equipped with an air conditioning system, temperature and humidity monitoring, an uninterrupted power supply, a fire detection and suppression system, and access control.

b) The NAO noted that DoE relies on MITA for regular backup of data, in respect of data residing on shared network drives and of Government email accounts, whilst DoE officers use the shared network drives, as well as external portable hard drives or pen drives to backup data. The NAO recommended that the DoE revises the current backup procedures adopted by DoE officers and issues clearly defined guidelines or policy.

c) Given the need for a standard operating procedure to cover confidential access to audit logs of DoE systems, by DoE senior management, the NAO recommends that such a document is drafted and adhered to by DoE.

d) Given the use of personal portable and mobile devices within DoE's premises, the NAO recommends that DoE management drafts, formalises and circulates a suitable policy governing the use of such personal portable and mobile devices within the Department's offices/premises.

Chapter 4 includes a review of the principal IT software applications, as well as the DoE's website and use of social media. The following are the key findings and recommendations included in this chapter:

a) In terms of the provision of maintenance and support of the DoE website, the NAO strongly recommended that this should be covered by a service level agreement between the third-party contractor and IMU-MFED/DoE, to ensure that any current and applicable terms and agreements are formalised into a legal document.

b) The NAO also suggested that system programming manuals for the Examinations Management System (EMS) application should be made available, and DoE and IMU-MFED should ensure that these are being kept up-to-date.

c) Given the ICT investments made by MFED, the NAO recommended that DoE management discusses and liaises with IMU-MFED to get a thorough overview of the existing pool of MFED's education IT systems, which may hold valuable data of relevance to the further automation and facilitation of DoE business process and functions. The DoE management may then consider obtaining access to such data or introducing such systems at the Department as required, with the aim of increasing efficiency.

d) This Office strongly recommended that the DoE considers enhancing its reach and accessibility to its clients and the community, through the use of social media platforms popular for interacting with the general public.

Chapter 5 tackles information security, IT risk management, including business continuity and disaster recovery, as well as security awareness related training at the DoE. The following are the key findings and recommendations included in this chapter:

a) Given that the DoE was preparing to relocate its offices to a new site subsequent to audit testing, this Office recommended the following:

- All efforts must be made by the Department to ensure that as a minimum, the same level of physical access controls are present in the new site.

- With respect to the installation of the video surveillance system at the new site, the DoE should ensure that the same level of controls relating to the storage, retention and access to the Closed-Circuit Television (CCTV) (video surveillance) footage, are maintained when settled at the new offices.

- DoE should ensure that adequate fire prevention and suppression systems are installed at the new office location, whilst ascertaining that these systems are adequately and regularly inspected and serviced, and the necessary training is provided to selected DoE members of staff.

b) The NAO recommended that the DoE drafts a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) which would include the possibility of using an alternative site (such as an office within an MFED building) to access DoE systems, which are hosted at MITA, should the DoE offices be unavailable due to a disaster.

c) The NAO recommended that the DoE management organises IT security awareness training sessions for its personnel on a regular basis so as to increase awareness amongst its employees on possible IT security risks.

Chapter 1| Introduction

This chapter provides background information on the subject under review and sets the context for the audit. It details the audit scope and objectives, and describes the audit methodology followed in attaining them, and concludes with a brief overview of each chapter in this report.

1.1 Background

The Department of Examinations' (DoE) mission statement states that its purpose is "*to administer local and overseas examinations that fairly and fully allow demonstration of candidates' learning.*"

The DoE's functions and responsibilities include managing examinations for induction into the Public Service, Public Corporations and commercial partnerships in which the State has majority shareholding; intra-service written examinations; and examinations for the issue of Local Licences. The DoE also acts as an agent for local and overseas examining bodies responsible for the award of Academic, Vocational and Professional Qualifications. Its clients/customers include school-leavers, mature students, educators, education administrators, examining bodies and the general public[1].

The DoE, which forms part of the Ministry for Education (MFED) (previously Ministry for Education and Employment (MEDE)), is headed by a Director, who acts as Registrar of Examinations (for Local Public Examinations), and is answerable to the Board of Local Public Examinations (whose Chairperson and members are appointed by the Minister)[1], and to other respective Examination Boards with regard to other examinations held by DoE.

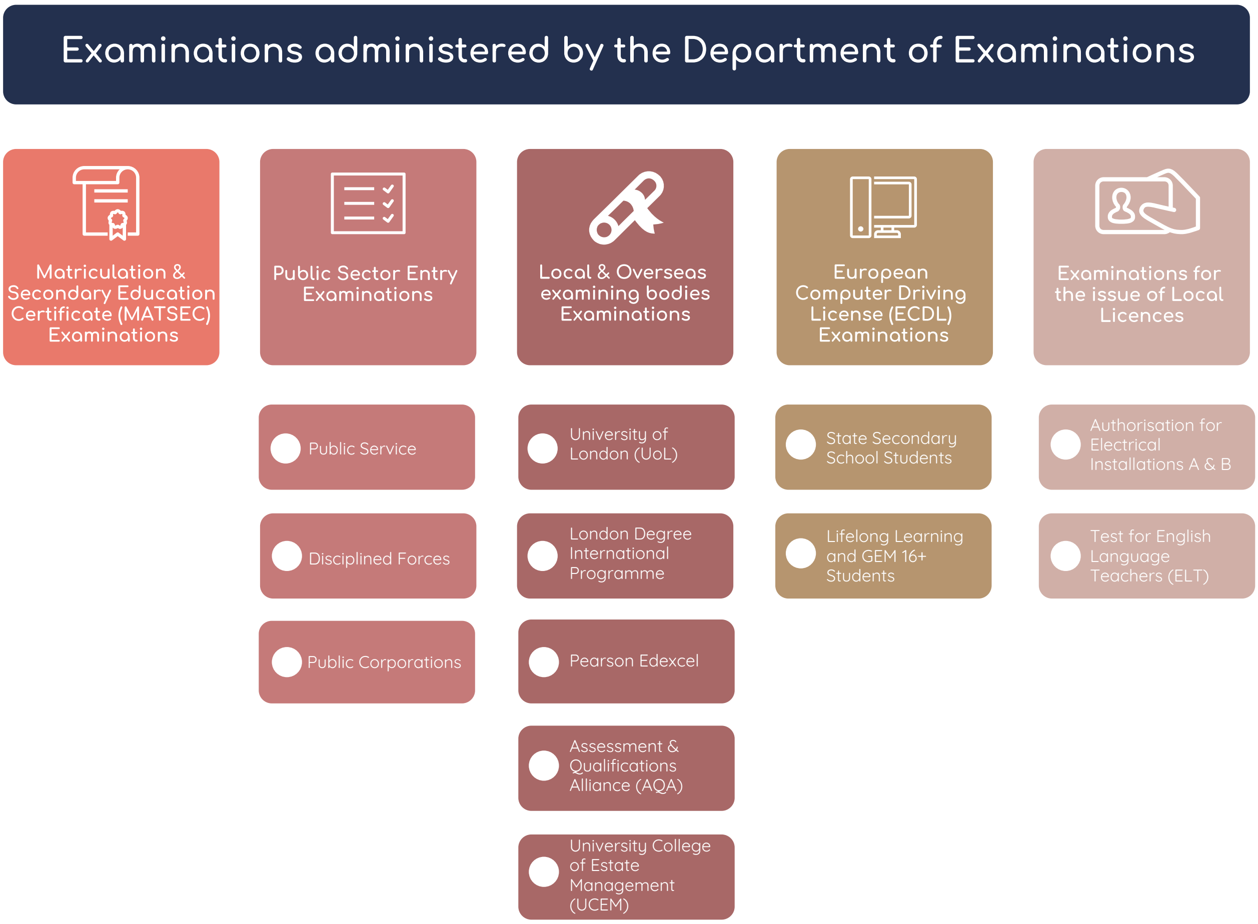
The department comprehends the importance of Information and Communications Technology (ICT) in today's society, its effect on public expectations, and the crucial role it plays in Government's business processes and operations, and, to this extent, in recent years, the DoE has invested towards digitising aspects of its services. In fact, MFED has reported, on a number of instances, the increase in local candidates submitting their applications electronically/digitally[2], whilst also having recently launched a new website[3], amongst other recent initiatives.

[1] https://myexams.gov.mt/about/

[2] MEDE Annual Report 2019

[3] https://myexams.gov.mt/

In this context, this Information Technology (IT) Audit sought to examine the current state of the ICT within the DoE to identify any potential risks, and through this report, document the observations, and make the necessary recommendations to mitigate those risks. All resulting findings and recommendations are contained within this report, which is issued by the IT Audit and Operations Unit with the National Audit Office (NAO). Eventually, DoE Management could then address and tackle the issues raised and highlighted by this Office in this report, mainly by implementing suitable remedial measures, in line with, or surpassing, the recommendations put forward by the NAO in this report.



Examinations administered by the Department of Examinations

- Matriculation & Secondary Education Certificate (MATSEC) Examinations
- Public Sector Entry Examinations
  - Public Service
  - Disciplined Forces
  - Public Corporations
- Local & Overseas examining bodies Examinations
  - University of London (UoL)
  - London Degree International Programme
  - Pearson Edexcel
  - Assessment & Qualifications Alliance (AQA)
  - University College of Estate Management (UCEM)
- European Computer Driving License (ECDL) Examinations
  - State Secondary School Students
  - Lifelong Learning and GEM 16+ Students
- Examinations for the issue of Local Licences
  - Authorisation for Electrical Installations A & B
  - Test for English Language Teachers (ELT)

1.2 Organisation Structure

During the course of this IT audit, the DoE was primarily operating from its offices situated at the Mall, Floriana, Malta. The building was shared with another Government (MFED) entity, namely, the Directorate for Learning and Assessment Programmes (Curriculum Department). Nevertheless, towards the end of this IT audit, the NAO was informed by DoE senior management that they were in the process of relocating their main office to a new site.

The DoE also has a satellite branch office located at Victoria, Gozo, principally to cater for residents of this island, and amongst other services, also assists with services which cannot be physically provided by Matriculation and Secondary Education Certificate (MATSEC) Examinations Board in Gozo.

Furthermore, the DoE administers three examination centres, namely St. Elmo Examinations Centre[4], Valletta, Malta, Gozo Examinations Centre[5], Victoria, Gozo, and St. Elmo Primary School Fourth Floor, Valletta, Malta. In addition, periodic use of various other Government, University or Church schools/colleges and examination facilities[6] is made by the DoE to aid in executing its functions/duties.

In terms of setup[7], the DoE operates through three operational units (Local Public Examinations section, MATSEC and ECDL section, and Foreign and Petty Examinations section) and two administrative departments (Accounts, Human Resources & General Administration section, and Reception), apart from the Gozo Examinations Branch, already indicated above (which is treated as a separate unit).

All units are headed by a Principal or Senior Principal officer (excluding Reception) and fall under the responsibility of the Assistant Director, who is answerable directly to the Director DoE.

[4] Some halls/rooms in this complex are currently not in use, due to structural/refurbishment works being carried out by Foundation for Tomorrow Schools (FTS) (as at audit date).

[5] This venue is also used for examinations by the University of Malta and Bart's Medical School, apart from occasional use for training of educators.

[6] https://myexams.gov.mt/venues/

[7] The DoE organisation chart, as at beginning of Q2 2021, is annexed in Appendix A.

1.3 Workforce Distribution and Work-Life Balance Measures

The DoE workforce is made up of 28 employees[8] of which four are posted at the Gozo branch.

The total DoE workforce distribution, classified in Managerial/Administrative/Clerical, and Non-Clerical grade categories, is as follows:

Management/ Administrative/ Clerical	Senior Management (Director & Assistant Director)	2
	Senior Principals	1
	Principals	5
	Assistant Principals	5
	Executive Officers	4
	Clerks / Assistant Clerks	3
	Other (Assistant Manager, Admin Support Officer, Care Worker, Receptionist)	4
Non-Clerical	Messenger Driver	1
	Cleaner	3

Of these employees, four have been engaged through the Community Worker Scheme, whilst another is on loan at DoE from a separate Government entity.

All DoE employees are employed on a full-time basis, including the two Senior Management officials.

[8] NAO acknowledges that staffing is a dynamic process. Figures are as provided by DoE as at audit period, circa beginning of Q2, 2021.

28

Full-Time Basis Employees

0

Contractual Basis Employees

0

Part-Time Basis Employees

The COVID-19 pandemic in 2020 brought about the overnight adoption of teleworking facilities for most of the DoE employees, who had to work from their homes in line with the Health Authorities' recommendations. In order to ensure that employees could easily continue working remotely from their homes, all officers were equipped with laptops, and most had access to Virtual Private Network (VPN) facilities to enable secure access to key DoE systems from outside the office. Furthermore, calls to office telephone lines were automatically diverted to personal home/mobile phones. This situation also meant that on occasion, internal DoE documentation had to be taken to the employees' homes for work purposes.

The following is a breakdown of family-friendly measures being availed of by DoE employees as at audit date, which had drastically changed post the COVID-19 pandemic peak:

8

Flexible Hours Employees

3

Teleworking Employees

4

Reduced Hours Employees

1.4 Legislation

The Education Act (Chapter 327, Part XI (Miscellaneous), para. 125)[9] establishes the office of the Registrar of Examinations, who is designated as the competent authority for the purposes of the same Article. The NAO was further informed that the DoE does not operate directly under any other additional legislation or legal publication (Acts of Law, Bills or Legal Notices).

Furthermore, as the DoE acts on behalf of various foreign examination boards, such as the University of London (UoL)[10], Edexcel[11], and Assessment and Qualifications Alliance (AQA)[12], as a licensed examination centre, it is also bound to follow the regulations of each respective Examination Board.

1.5 Audit Scope and Objectives

The scope of this IT audit was to analyse and review the ICT within the DoE, including, IT management, infrastructure, operations, security, and software applications. Such Government investments were scrutinised, in a risk-based manner, to determine whether the necessary level of controls exist, at departmental level, to ensure that assets are safeguarded, resources are used efficiently, data integrity is maintained, and organisational goals can be achieved effectively.

In this regard, this IT audit sought to review and assess the level of controls in place, mainly those relating to the IT network infrastructure (such as firewall and network protection, etc.), IT security (including operating systems patches and updates; anti-virus, anti-malware and threat protection updates; etc.), and software applications (such as login credentials, audit trails, data backups, data confidentiality, etc.), amongst other key areas.

Moreover, this IT audit sought to review the current state of IT operations and systems within the DoE, and elicit any potential areas of risk to the DoE, its functions and operations, and/or its clients.

Thus, through this report, the primary objectives were to document and summarise all the information gathered from various sources and identify any areas of concern; determine whether the DoE's IT setup facilitates operations in an effective, efficient, and economical manner; list all the observations, findings and any potential risks identified; and make the necessary recommendations to mitigate those risks.

Notwithstanding the above, it is to be noted that, given the aforementioned scope, the review of the selected software application/s does not constitute an in-depth information systems audit, which mandate would typically be carried out as a stand-alone review of a given information system.

[9] https://legislation.mt/eli/cap/327/eng/pdf
[10] https://london.ac.uk/
[11] https://qualifications.pearson.com/en/home.html
[12] https://www.aqa.org.uk/

1.6 Audit Methodology

Prior to undertaking this audit, the NAO initially gathered and assessed any publicly available information on the subject matter. Once the scope of this exercise was defined, an overview of the IT audit process was outlined, through an introductory meeting held with DoE senior management. A request for preliminary information/data was made by the NAO and forwarded to the auditee.

This was followed by an on-site meeting whereby the NAO audit team were briefed on the main operations, functions and processes at the Department, and were then given a familiarisation walkthrough to acquaint themselves with the DoE's setup and environment first-hand, from an IT perspective.

Subsequently, a detailed pre-audit questionnaire was compiled by NAO and eventually completed by the DoE. The documented response provided comprehensive insight, and further enhanced the audit team's understanding of the IT setup and operating environment at the DoE.

Following a risk analysis and review of available information and feedback submitted, audit testing commenced. NAO's testing was segmented so as to verify and assess various aspects of IT including, IT management (strategy, objectives, internal structures, etc.), infrastructure, operations (including functions and processes), security, and software applications (including usage and objectives), amongst other areas.

Given that this was conducted during the COVID-19 pandemic, and that the Department was undergoing a relocation during the same period, the audit team had no option but to rely heavily on documentation and additional information provided by the auditee, as well as online meetings and correspondence, whilst keeping on-site audit fieldwork (physical verifications, meetings and interviews) to a minimum.

As far as possible, the methodology adopted by NAO relied on the Control Objectives for Information and related Technology (COBIT) set of best practice guidelines[13], created by the Information Systems Audit and Control Association (ISACA) for IT management and IT governance, and includes an overview of business continuity and disaster recovery measures.

1.7 Audit Period

Preliminary research, planning, meetings, interviews, analysis, testing, review and reporting were carried out during the period December 2020 to June 2021.

[13] https://www.isaca.org/resources/cobit

1.8 Structure of the Report

This report comprises six chapters in total, with all but the last chapter documenting the information collected and highlighting relevant findings and recommendations. The next five chapters are structured as follows:

- Chapter 2 covers the IT management outlook and reviews the management of ICT resources at the DoE.
- Chapter 3 deals with controls concerning the IT infrastructure and IT operations at the DoE.
- Chapter 4 includes a review of the principal IT software applications, as well as the DoE's website and use of social media.
- Chapter 5 tackles information security, IT risk management, including business continuity and disaster recovery, as well as security awareness related training at the DoE.
- Chapter 6 lists the DoE management comments submitted and depicts the agreed recommendations implementation schedule.

1.9 Acknowledgements

The NAO would like to express its appreciation to all the DoE key stakeholders who were involved in this IT audit, including the Director DoE, Assistant Director DoE, and Principal Officer responsible for IT, as well as IMU-MFED and MITA officers, for their time and assistance throughout this exercise. The NAO commends the forward-looking perspective and proactive approach adopted by the DoE in modernising/digitising their services, which was evidenced throughout the audit.

Chapter 2| IT Management

This chapter covers areas related to IT governance, from strategy and budgeting, to procurement and disposal of ICT resources/services, to asset management and supplier/contractor management. It also looks into the availability of ICT support, and the provision of ICT training to DoE employees.

2.1 IT Strategy and Budgeting

During the course of this IT audit, this Office was informed that the DoE does not have an IT Strategy, nor specific capital or recurrent ICT Budget allocations (or any votes) for ICT infrastructure. Referring to an IT strategy, the DoE indicated that it refers to and follows the guidelines set out by MITA and Information Management Unit (IMU)-MFED. Likewise, regarding the ICT Budget, the DoE indicated that any such budget is planned and determined through IMU-MFED.

Moreover, DoE also has funds available for the procurement of scanning pens, to be used by examination candidates with special access arrangements, during specific examination sessions. Meanwhile, in terms of major projects with an ICT component planned for the near future, at the time of IT audit testing, DoE was developing a revamped and upgraded Examinations Management System (EMS). This Office was informed that this project is being financed by IMU-MFED, and DoE indicated that works were already in progress during the audit and were in fact successfully completed by quarter two 2021.

2.2 IT Procurement, Maintenance and Disposal

The NAO was informed that in terms of procedures adopted for the procurement, maintenance and repairs, and the disposal and replacement of IT hardware and equipment, DoE is guided by IMU-MFED direction and follows MITA procedures, whilst specifically relying on the support provided by IMU-MFED.

Specifically, procurement of any IT hardware and equipment required by DoE is made by IMU-MFED on their behalf, after the DoE has made its requests, and these have been processed by IMU-MFED.

Meanwhile, all hardware is maintained and serviced through IMU-MFED, whilst technical officers are also sent on-site by IMU-MFED to tackle any issues related to damaged or faulty DoE equipment, and follow up with the required action. Conversely, MITA staff intervene directly online to tackle any potential issues encountered by DoE officers on software covered by MITA support services.

With regard to the disposal of IT hardware and equipment which is obsolete or beyond economical repair, the Chief Information Officer (CIO) IMU-MFED is notified once a substantial amount/volume of such items has accumulated. In turn, technical officers are sent on-site to duly inspect these unusable/unserviceable items. An inventory is also drawn up listing details of this equipment, and authorisation for disposal is then granted after the request has been reviewed by IMU-MFED. Devices are then formatted by IMU-MFED officers whilst Request for Service (RFS)s are raised for the deletion of accounts and access is revoked. Finally, DoE may then carry out the necessary steps to dispose of the items accordingly. The NAO was notified that prior to this IT audit, the last disposal process was carried out in November 2020. The DoE did not confirm the process adopted for wiping data when transferring or disposing of IT assets.

Similarly, in reference to systems development life cycle, i.e. the planning, development, acquisition, testing and implementation of software applications, this Office was informed that the DoE follows directives issued by the CIO IMU-MFED, adding that it is the latter which determines the standard to adhere to for the development life cycle of all IT systems in use, whilst taking into consideration the evolving business processes of the Department. In this regard, DoE maintained that the implementation or upgrade of major software applications requires technical planning beforehand, internal discussions with IMU-MFED and MITA as necessary, as well as financial planning to secure the necessary funds for such projects, although such funds usually emanate from IMU-MFED.

2.3 IT Asset Management

The NAO was informed that the IMU-MFED maintains and updates the inventory of all IT hardware and software applications in use by DoE, as is done with all other Departments within MFED. Furthermore, the NAO was also informed that the DoE does not have access to the IT inventory data.

A similar situation was reported to NAO with regard to the management of DoE software licences, where it was stated that this is also within IMU-MFED's remit, which in fact keep track of all software licences in use by DoE. The latter does not hold any inventory of these intangible IT assets.

2.4 IT Supplier/Contractor Management

During the course of the audit, the NAO observed that the DoE maintains a number of ICT related service level agreements or maintenance contracts with respective third-party vendors/service providers. The principal ICT operation covered by such agreement at DoE level is the maintenance and support of the EMS application[14].

[14] With regard to the VMS application and the DoE website, the NAO was not provided with similar service level agreements for these IT services, as will be explained further on in Chapter 4 of this Report.

Further to the above, the NAO was informed that DoE has one full-time officer, in the grade of Principal, who is responsible for coordinating and monitoring these contracts. This officer is responsible to handle related tasks and issues, liaising with the respective third-party vendor/service provider, as well as IMU-MFED, acting on behalf of DoE.

Upon examining the service level agreement covering the provision of maintenance and support for the EMS, the NAO observed that the current/active contract is an extension of the original agreement between IMU-MFED and the contractor, although the copy provided to this Office was not signed and endorsed by either party. This agreement provides clear and detailed conditions and procedures, service level indicators with response times and resolution of incident times, procedure for fault reporting, and provision of management reports. On the other hand, the contract does not define when penalty charges may be applicable.

A review of the means of communication with this respective contractor for support purposes are included in the next section of this Chapter.

2.5 IT Team/Unit and IT Support

Early on during the course of this audit, this Office observed that DoE does not have an IT unit/team, or specific IT officer solely focused and responsible for ICT matters.

Instead, as already indicated throughout this report, DoE has a full-time officer, in the grade of Principal, who in addition to her normal office duties, is entrusted with dealing with day-to-day ICT matters. In fact, this technical coordinator offers support and assistance to all members of staff, including senior management, whilst liaising and coordinating with CIO IMU-MFED, as well as MITA, when, for example, members of staff require access to certain software applications, or when a higher level of support which goes beyond her level of expertise is required. The NAO was also informed that all such DoE communication with IMU-MFED, MITA, as well as third-party vendors/service providers, is always channelled through this officer, who follows procedures/instructions accordingly, and keeps track of all communication and support transactions carried out.

In this regard, the NAO was informed that, with respect to EMS, the above-mentioned support transactions are raised and followed through a specific ticketing system (called MIRS). In terms of procedures, should an issue arise, a ticket is immediately opened by this officer. Each ticket is numbered so its progress can easily be tracked. This system facilitates communication with the contractor, as it enables the immediate reporting of any arising issues.

Furthermore, DoE added that apart from the above process, the officer also relies on email correspondence (via Microsoft Outlook) and online meetings (via Microssoft Teams) so as to communicate with the DoE's other contractors/service providers and ascertain that support is always provided.

2.6 IT Training

When queried about ICT training, the DoE explained that whenever new software applications are introduced within the Department, senior management ensures that the relevant officers are provided with the necessary training. Typically, this would be in-house training, although there were also instances when training was provided by the service provider, either delivered on-site or at a designated training centre.

In this regard, DoE relayed a few key examples to substantiate this. Namely, with the introduction of the EMS in 2011/2012, training was provided by the vendor to all members of staff, whilst dedicated training and support were also provided by the same supplier whenever major changes/upgrades were implemented on this system, or when new system users were engaged by DoE. Meanwhile, with the launch of the new DoE website in 2019, four officers, including two senior officials, attended a brief training session (meeting), organised by the service provider at their offices, enabling them to perform website updates with limited outside assistance. Similarly, upon the introduction of the new Government corporate financial management solution (CFMS) (replacing the departmental accounting system (DAS)), four officers were each provided with three training sessions by a third-party.

Upon enquiries, DoE clarified that in the above scenarios, a training certificate is not usually provided.

2.7 Observations, Conclusions and Recommendations

IT Strategy and Budgeting

The DoE management should seek to discuss its strategic plans and annual budget requirements with IMU-MFED, with the aim of consolidating the IT elements in these plans, and eventually draw up a specific DoE IT Strategy and annual IT Budget, in line with those at IMU-MFED.

IT Procurement, Maintenance and Disposal

With reference to the transfer or disposal of the Department's IT equipment, the DoE is to ascertain that such IT equipment is securely data wiped before the transfer or disposal of this equipment, so as to prevent the loss of any sensitive information and/or unauthorised access to such information.

IT Asset Management

In relation to the Department's IT hardware and software inventories and the management of software licences, the DoE should ensure that it is given read-only access to the related inventories of both tangible and intangible IT assets, to be in a better position to plan its future IT needs.

IT Supplier/Contractor Management

Regarding the Department's service level agreement with a third-party contractor covering the maintenance and support of the EMS application, the DoE should ascertain that a signed copy of this agreement is readily available.

Furthermore, the NAO recommends that the DoE and IMU-MFED carry out regular/periodic reviews of the standing service level agreements to ascertain that the conditions of such agreements are being adhered to by the third-party contractors, such as adhering to service response times, and provision of access to the latest version of the system's source code, where applicable. Besides, DoE should also consider the inclusion of relevant penalty clauses within these contracts.

IT Team/Unit and IT Support

In the absence of a dedicated IT team/unit at the DoE, and the continued reliance on the support of IMU-MFED and MITA, the NAO suggests that the DoE management should look into the possibility of engaging a full time IT officer who shall be responsible for the management of the Department's IT requirements.

Chapter 3| IT Infrastructure and Operations

This chapter details the IT infrastructure setup at DoE, and reviews the other key aspects of IT operations within the Department.

3.1 IT Infrastructure

As stated further on in this Chapter, the DoE is connected to MITA's Corporate Domain and the Malta Government Network (MAGNET)[15], therefore accessing MITA's server related services, such as software application hosting, provision of shared network drives, email and internet services, as well as access to Government corporate systems such as the Common Database (CDB), the Corporate Data Repository (CDR) and CFMS.

The IT infrastructure at DoE was primarily made up of the following hardware, software, network equipment and shared network drive server folders amongst others.

3.1.1 Hardware

The IT hardware in use at DoE consisted of the below listed equipment:

Laptops	32
Monitors	9
Multi-Function Printers	7
Interactive Whiteboards	6
Scanning Pens	30

[15] MITA's Malta Government Network (MAGNET) is the Government's secure and private wide area network that interconnects all Government Ministries, Departments, Entities and Embassies, and provides connectivity to the Core Network within MITA Data Centre.

With regard to hardware being utilised by the DoE, the majority of users are provided with laptops as per Ministerial policy, which enables mobility in view of teleworking requirements, whilst an additional small number (seven) of laptops are also available for use by examination candidates with special access arrangements. Nine monitors are utilised on-site within the offices to be used as extended displays. DoE offices are also equipped with seven multi-function printers to cater for office printing requirements and periodic high-volume printing jobs carried out internally. DoE also makes use of six interactive whiteboards for presentation and communication purposes. As previously indicated, 30 scanning pens were also procured to be used by examination candidates with special access arrangements, during specific examination sessions.

3.1.2 Software

The IT software applications in use by DoE primarily comprised of the following:

- Examinations Management System (EMS) – a custom, locally built software application, used to store and manage data in relation to examinations held by the DoE.

- Visitors' Management System (VMS) – an off-the-shelf, locally procured software application, used to electronically register and manage clients and visitors of the DoE offices.

Moreover, DoE uses a number of other applications (mostly off-the-shelf) which, in conjunction with the other software applications listed here, are used to process, store and maintain a considerable amount of data as part of its daily functions.

DoE utilises a number of third-party examination applications, specific to some of the examinations it routinely holds[16], and also has access to Government's CDB and CDR databases, as well as the eID repository. DoE also confirmed that the Department has access to the required online facilities to allow online payments, such as internet banking facilities.

On an administrative level, DoE utilises the Microsoft Office 365 suite to automate office tasks (such as documents, spreadsheets, etc.). In addition, like other Government Departments, DoE also makes use of the DAKAR package with modules for human resources, leave, and performance appraisals; and the CFMS for accounting purposes.

Finally, with regard to the laptops at DoE, in terms of operating systems, all devices in use are running on Microsoft Windows 10.

[16] These include applications in relation to Edexcel, AQA and ECDL examinations.

3.1.3 Network

The NAO was informed that the DoE is connected to MITA's Corporate Domain and the MAGNET as its primary network connection. All the main DoE services and software applications are accessed through this network. Each authorised DoE user is provided with his/her own unique login credentials to connect their workstation to MITA's Corporate Domain and access the related available services. DoE also pointed out that monitoring and controls, such as firewalls, web filtering, malicious code detection and measures against phishing, are handled by MITA.

Furthermore, during the course of this audit, this Office observed that a third-party wireless network connection was also available on all the floors within the building housing the DoE offices in Floriana. The NAO was informed that this Wi-Fi connection was shared by DoE with the Directorate for Learning and Assessment Programmes (Curriculum Department) housed on the second floor of the same premises. The network was password protected, and DoE has indicated that this service is utilised by DoE and Curriculum Department staff, as well as authorised guests and visitors. This network is for inhouse use by DoE staff only.

3.1.4 Shared Network Drive Server Folders

The NAO observed that DoE also makes of use of MITA's dedicated shared network drive server folders. The server folders are part of MITA's File Share Service Packages provided to its clients (i.e., Government Departments, Ministries, Entities, etc.), and provide a specific storage space on MITA's servers allocated for use by DoE. The server folders are accessed and shared by authorised DoE users only, who are assigned the appropriate rights by IMU-MFED through MITA. This ensures that access to specific files or folders on this network drive is restricted to the owner and relevant authorised user/s only.

DoE stated that data kept and maintained by its staff on these server folders comprises of various databases/spreadsheets, DoE templates, and other DoE operational and business-related data.

Following enquires made by NAO, DoE claimed that these server folders are also regularly used by DoE officers as a means of manually creating copies of data or files which are shared internally, rather than residing solely on individuals' laptop drives.

3.1.5 Servers and Data Storage Equipment

This Office observed that DoE relies heavily on MITA infrastructure for its functions/services, as well as the backup and disaster recovery processes provided by MITA.

Consequently, an on-site review at DoE premises carried out during the audit showed that DoE does not have a dedicated server room, nor a server, nor any network attached storage devices at its offices.

Thus, the provision of the above-mentioned facilities are not deemed to be essential or a requirement for DoE's operations. In fact, the DoE benefits from a higher level of flexibility afforded by the fact that related server folders can be accessed through the Government network or secure VPN connections. The latter was of particular importance for DoE during the COVID-19 pandemic.

3.1.6 Network Cabinet

During its on-site review, the NAO observed that, in terms of equipment, DoE has a network cabinet, installed on site at its office in Floriana.

The NAO commends the fact that, in the absence of a dedicated room on the present premises, the network cabinet was not placed amidst a corridor or similarly highly trafficked area, and was in fact sited in a corner within one of the offices located on the first floor. This room/office could be locked, thereby limiting physical access to this essential equipment.

Moreover, temperature and humidity levels inside this office (where the network cabinet is sited) could be adjusted and maintained manually, through the use of an adequate air-conditioning unit, which had the facility to control both. However, no additional temperature/humidity monitoring equipment was observed or indicated in this room/office.

Similarly, DoE confirmed that no fire prevention or detection equipment were currently present in this room/office, although it was indicated that a carbon dioxide type fire extinguisher was installed and available in the proximity of the network cabinet.

Nevertheless, this Office was pleased to be informed by DoE that, given that the Department is set to change venue soon, it is being planned that a separate room will be set up to house the Department's network cabinet. DoE further claimed that it is planned that this dedicated room will be equipped with all the requisite safety and security equipment.

In the meantime, it was confirmed that at present, there aren't any uninterrupted power supplies connected to the network switches, to provide the necessary temporary power in the event of a power outage.

Furthermore, the audit team also noted the absence of structured cable management within this network cabinet, which poses various problems when handling future troubleshooting of network related issues.

3.2 Patch Management

The NAO was informed that patch management procedures and the deployment of service packs, security patches, hotfixes, etc. on DoE equipment, fall under the remit of IMU-MFED and MITA.

This implies that, on one hand, the IMU-MFED's role is to monitor and ensure that all devices are duly updated with the latest software patches, whilst all essential software updates, such as Micosoft

Windows updates, are pushed, delivered and installed automatically by MITA. This will ensure that all DoE equipment is always kept up-to-date.

3.3 File/Folder Access and User Account Management

The NAO noted that, DoE has a setup where files/folders can only be accessed by network users having the requisite access rights/permissions, as a means to control access to data or computer resources, and prevent unauthorised access to these assets.

It was explained that assignment of file/folder permissions, as well as user access rights to ICT software applications, and creation and deletion of user accounts, etc., are carried out by IMU-MFED. DoE added that one of its officers, in the grade of Principal, is responsible for coordinating these tasks with IMU-MFED accordingly.

With regard to logins/passwords used by officers with IT administrator rights, DoE claimed that these are only used by authorised users and are not passed to or shared with other unauthorised members of staff or third-parties.

In terms of user accounts, DoE indicated that the users' passwords used to access DoE IT infrastructure are subject to MITA's password policies and procedures, hence password expiry after a defined period, password history retention and blocking reuse of previously used passwords, amongst others features.

3.4 Backups and Recovery of Data

As some of DoE's software applications are hosted on MITA infrastructure, specifically on MITA's Segregated Hosting Environment, the Department relies on support provided by IMU-MFED and MITA. Nevertheless, access to the above-mentioned environment, and servers therein, is governed by MITA's clients, in this case IMU-MFED on behalf of DoE, or the third-party contractor/s acting on behalf of IMU-MFED. This implies that IMU-MFED, or the third-party contractor acting on its behalf, is responsible for regular backup of data, periodic testing of backups, and recovery of data from backup as necessary, in respect of data residing on shared network drives and of Government email accounts.

Nevertheless, the DoE added that each of its officers is responsible to backup his/her own local work data, and in this respect, the shared network drives are themselves regularly used to backup data, as already indicated earlier on. Additionally, the NAO was also informed that DoE users are also performing data backups, either on their device's own hard disk, or on external portable hard drives or pen drives.

3.5 Internet and Electronic Mail

The NAO observed that even though DoE does not have its own internal, formally documented policies governing the use of internet and email, however, DoE follows MITA's Government of Malta

ICT (GMICT) Internet and Electronic Mail usage policies[17] in this regard. The same applies to DoE's adherence to MITA's web filtering policy.

In this regard, DoE elaborated that all Uniform Resource Locators (URLs) or websites that have been blacklisted by MITA are inaccessible to its members of staff. However, in the event that DoE should deem that access is required to a particular (partially or completely) blocked website for work purposes, the matter is raised by the Director DoE with IMU-MFED and MITA.

With regard to generic email accounts, the DoE indicated that the Department currently has one such generic email account: myexams@gov.mt. The NAO was informed that this account is used to provide general customer care, with the possibility of redirecting queries/questions to the related DoE officer. DoE added that the generic email account supplements the online platforms used by the Department, such as the Recruitment Portal, however, it is not directly used for the submission of applications or payments related to examinations. In this regard, the audit team was informed that the Department does not currently keep a log of support provided through this channel. The generic email account is administered by the Assistant Director DoE, and this can be accessed by six members of staff. Support provided through this generic email account is done during office hours.

3.6 Audit Trails

As DoE relies heavily on MITA infrastructure for its functions/services, the Department depends on audit logs set up and maintained by MITA at server level. In this regard, audit logs for project folders (in use by DoE) are available as part of MITA's File Share Service Packages. However, whilst these audit logs are available, these are not provided automatically to any client, and can only be accessed by suitably authorised staff. Nevertheless, IMU-MFED may contact MITA, on behalf of DoE, to request specific audit trail reports.

With respect to DoE's information systems and applications, hosted on MITA's Segregated Hosting Environment, access to this environment (and servers therein) is governed by the client, i.e., IMU-MFED on behalf of DoE, or the third-party contractor/s acting on behalf of IMU-MFED. In this regard, this means that the servers within this environment are installed, configured, managed, and operated solely by the client, and thus it is implied that it is the client's responsibility to configure monitoring tasks such as audit logging, etc. This was corroborated by DoE, which claimed that any audit trails of the key software applications are set up and monitored by IMU-MFED. DoE also stated that the Department does not have any access to such audit trails/privileged information.

Furthermore, following enquiries by this Office, DoE specified that there haven't been any recent instances where DoE management had to refer to or request access to such audit trails. This was also confirmed by MITA, which stated that it did not receive audit trail requests (from MFED) specifically in relation to project folders pertaining to DoE.

[17] https://mita.gov.mt/portfolio/ict-policy-and-strategy/gmict-policies/

3.7 Portable and Mobile Devices

With regard to the use of personal portable and mobile devices within the DoE offices, the auditee confirmed that personal devices are unable to access any resources on the Department's IT network connected to MAGNET[18]. In this regard, this Office is pleased to note that non-official or personal devices cannot be connected to this network as these may pose various security risks and threats, especially if their integrity has already been compromised when connected to different networks.

On the other hand, with access to a valid network password, such personal devices may connect to DoE's secondary third-party wireless network when on site.

DoE added that it does not have any internal formally documented policies on the use of such personal portable and mobile devices within its offices.

3.8 Multi-Function Printers

The audit team was informed that the multi-function printers installed throughout the DoE's offices and connected to the Department's IT network, are all access controlled. In fact, the NAO was pleased to note that these are all password/passcode protected, with an individual password/passcode generated for each DoE officer. This ensures that access to print jobs is restricted to the relevant user only.

3.9 Cloud Computing

In response to enquiries made during the course of this audit, the NAO was notified that all DoE officers have Microsoft OneDrive for data storage related to their work, whilst the Department uses Microsoft Sharepoint for the digitised registers used in relation to the issue of provisional certificates.

3.10 Observations, Conclusions and Recommendations

IT Infrastructure

As regards the networks to be used at the DoE's new offices, should DoE management decide to install a third-party wireless network at its new offices, the NAO recommends that such a network is completely segregated from the DoE's main IT network connected to MAGNET, and should only be accessed by authorised users through login and password provided by the Department. The NAO also recommends that this password is changed regularly, and adheres to current best practices related to passwords.

[18] However, some devices may access such network resources if the user has a CORP account and has necessary rights to use a VPN connection, on such device, thereby providing access these network resources.

With reference to the shared network drive server folders, the NAO suggests that all DoE officers make every effort to continuously use the network drives (personal, common, Projects Folder, etc., depending on the nature of the data) to save the data they are working on. This reduces the risk of losing valuable data should the user's laptop drive develop any critical faults. Furthermore, as these network drives are regularly backed up by MITA, this provides additional data security and peace of mind to the DoE.

In relation to the network cabinet to be utilised at the DoE's new offices, the NAO recommends that DoE management ensures that this cabinet is installed in a separate room, as well as being adequately equipped with an air conditioning system, temperature and humidity monitoring, an uninterrupted power supply, a fire detection and suppression system, and access control. Furthermore, the NAO also suggests that DoE management ascertains that all wiring within the cabinet is conducted using current best practices related to cable management, so as to facilitate the identification and troubleshooting of any network issues.

Patch Management

With reference to patch management procedures, the NAO suggests that IMU-MFED continue to monitor and ensure that all DoE hardware is duly updated with the latest software patches, thereby ascertaining that all DoE equipment is always kept secure, reliable, and up-to-date.

Backups and Recovery of Data

In relation to backups and recovery of data, the NAO recommends that IMU-MFED thoroughly reviews the current and informal processes adopted by DoE officers to backup their data, and formalises a suitable policy to provide guidance and ensure uniformity and adherence to current best practices relating to backups of data, thereby providing further security to DoE's digital assets.

Internet and Electronic Mail

With regard to the usage of Government's internet and email services, the NAO suggests that DoE management should ascertain that all its officers, especially new recruits, are fully aware of the applicable GMICT policies governing the use of these services.

Meanwhile, as regards the DoE's generic email account, the NAO recommends that the Department maintains a detailed log of the request for support (calls) received through this channel. Moreover, the NAO also suggests that the logs for a minimum period of six months (which should also include the summer period) are analysed. Should this analysis show a substantial number of requests for support, received through this generic email, outside working hours, DoE management should look into the possibility of extending this support service outside working hours, if deemed necessary.

Audit Trails

In relation to audit trails, the NAO recommends that the Department draws up and formalises standard operating procedures to cover confidential access to audit logs of DoE systems, by DoE senior management only, when the need arises. Moreover, the NAO suggests that such audit trails are occasionally scrutinised by DoE senior management to detect any unusual transactions.

Portable and Mobile Devices

With regard to personal portable and mobile devices, the NAO recommends that DoE management drafts, formalises and circulates a suitable policy governing the use of such personal portable and mobile devices within the Department's offices/premises.

Chapter 4| IT Software Applications

The scope of this chapter is to provide a high-level insight into the key IT software applications in use by DoE, namely, the EMS and the VMS, as well as the DoE's website and use of social media and networking platforms.

4.1 Examinations Management System

The Examinations Management System (EMS) is an online system used by DoE in relation to a number of local examinations (MATSEC and local public exams) and foreign examinations (UoL, Edexcel and AQA). The system is used for the storage of data (including personal data), keeping records relating to these examinations.

The EMS provides for the allocation of candidates, including those with access arrangements, and of invigilating staff within the centres/venues used for such examinations. The system also keeps track of all the hours worked by invigilators and supervisors, so that reimbursement can eventually be effected. The EMS also permits the registration of late applications, whenever this is required. The system was introduced by DoE in the period 2011/2012.

Though the system is owned by DoE, the Department clarified that the data in respect of local public examinations is jointly owned by DoE and the Board of Public Local Examinations. With respect to examinations conducted by DoE on behalf of other examining bodies, such as MATSEC examinations, the data owner is the third-party examining body (ex. MATSEC Board) and not the DoE.

The EMS, which is based on Microsoft .NET framework, is a dedicated, tailor-made web based software application intended for the specific needs of DoE. The software was developed by a local third-party vendor, and any enhancements and/or upgrades are carried out by the same service provider. DoE added that the service provider also provides maintenance and back office support. Additional support is also provided by IMU-MFED.

The NAO was also informed that the system is hosted on MITA's secure server facility, which has its own backup procedures.

In terms of access, the audit team observed that access to the EMS application (and any data stored therein) is restricted to authorised users/personnel only, via individual usernames and passwords. In terms of complexity, passwords need to be at least eight characters long, expire following the lapse of

90 days, and cannot be reused. Moreover, system access is blocked if a user unsuccessfully attempts to input incorrect credentials a specific number of times, resulting in the user's account becoming inactive.

The NAO was informed that, as at audit date, the majority of DoE personnel had access to this system. In this regard, the EMS is accessed by 23 members of staff, (including three members of staff in Gozo). Furthermore, the system can also be accessed by two supplier staff, four IMU-MFED staff, and two MITA staff for maintenance and support.

The NAO noted that the EMS has different access levels, according to the role of the user. This has been attained by creating twelve different user groups, each with different access rights, such that officers within each unit (of DoE) can only have access to the relevant section of the data.

It was also clarified that only DoE users/officers (fourteen) who are in charge of performing DoE processes in respect of specific examination boards (such as MATSEC, ECDL, UoL, etc.) have rights to delete records, and in these cases, only applications can be cancelled/deleted. Other data/records cannot be deleted.

Meanwhile, three other officers/user have been assigned administrator rights. DoE also stated that a DoE officer in the grade of Principal administers the system, and is responsible for user account management, high level maintenance, etc. Furthermore, senior management (the Director and Assistant Director DoE) have full access to the system.

With regard to users who retire, resign, or whose employment is terminated, the DoE claimed that the departmental coordinator, in liaison with IMU-MFED, ensures that these users' login credentials are removed and access to the system is disabled. On the other hand, unfortunately the NAO observed that the same is not true for users who are on maternity leave, prolonged leave or career breaks, whose access to the system is not temporarily disabled.

Upon enquiries, DoE also clarified that the third-party vendor has retained access to EMS so as to be able to provide any technical support related to patches, updates, retrieval of data, bug fixes, etc.

In terms of system audit trails, this Office was informed that these audit trails are maintained on every (database) table, with no time limit having been set for the time being, and hence, these audit records are currently being retained indefinitely. DoE also stated that these audit records are being kept by the system's third-party vendor/supplier.

DoE did not report any known bugs which had yet to be fixed during the initial stages of the audit. However, following audit testing, DoE later reported several issues relating to applications, payments, allocations, as well as loss of data, issues with functionality of the reporting system and other bugs. In one such example, at the time of audit testing, NAO was also notified that during the first quarter 2021, DoE was not being notified in any manner at their end that payments by candidates who were applying for examinations, had been made and settled. This occurred in spite of the candidates having successfully paid the examination fees and even received an acknowledgement. In this case, the NAO was notified that these issues were discussed with the third-party vendor to find a workaround, and patch/upgrade the system accordingly.

Following enquires made by the audit team, the Department claimed that these have occurred pursuant to the changes and upgrades in MITA's hosting infrastructure. Meanwhile, MITA stated that they were not aware of the above-mentioned issues at the time of enquiry. However, MITA also confirmed that as this application is hosted on their environment (whilst being administered and maintained entirely by the IMU-MFED, or the third-party supplier on the IMU's behalf), and as this (environment) is subject to changes and updates to MITA's underlying hosting infrastructure, thus, issues which affect software applications, may sometimes arise, pursuant to such changes and updates. Nevertheless, the NAO was informed that in such instances, MITA works with the client (and their contractor, as the case may be) to resolve such issues in the shortest time possible. This was also corroborated by DoE, which assured that the third-party vendor, as well IMU-MFED and MITA, always provide adequate support and resolve the issue/s when bugs are reported.

In the meantime, DoE indicated that during audit testing, works were already underway on an upgrade and revamp to the present system by the same third-party vendor, as noted earlier on in this report. NAO observed that this upgrade mainly included changes related to the migration to a newer version of the .NET framework, although DoE indicated that a number of enhancements were also being introduced. DoE stated that the system was being revamped to reflect changes to the department's business process that had already taken place, as well as changes that were envisaged to occur in the future, noting as an example, reforms taking place in MATSEC examinations, in line with the electoral manifesto, whereby candidates will be sitting for examinations in their natural schools rather than having to travel from one centre to the other to sit for their exams. Following IT audit testing, DoE confirmed that the upgrade was in fact successfully completed by second quarter of 2021.

Nonetheless, even though the Department did not comment whether a business process reengineering exercise had ever been carried out, DoE remarked that the EMS's lifecycle was determined by the department's evolving business process. DoE added that a list is being kept of what improvements can be introduced without negatively impacting the system. DoE also stated that there is also a plan for a new EMS, although no further information was provided at the time of the audit.

As already highlighted earlier on in this report, this Office observed that the provision of maintenance and support for the EMS is regulated by a service level agreement, which, amongst other aspects, covers service level indicators, response times and resolution of incident times, procedure for fault reporting, and provision of management reports. The NAO noted that the copy of the document supplied to the audit team contained no signatures of either party.

Moreover, as already mentioned in Chapter 2 of this report, the NAO noted that all support calls related to this system are logged in a specific ticketing system which assists in the follow up of the issues encountered.

The audit team was informed that programming manuals (i.e. source code and related software development documentation) for this software application are not available. In contrast, during audit testing, this Office was pleased to note that two DoE officers using the EMS have taken the initiative to draw up, and update, an in-house user manual of this system, complete with step-by-step instructions and various screenshots.

The NAO was also informed that, users were provided with on-the-job training, as well as dedicated one-to-one sessions, so as to familiarise themselves with this system and all its functionality.

The audit team observed that in terms of reporting functionality, the EMS application uses the Microsoft SQL Server Reporting Services (SSRS) and the SAP Crystal Reports software as a report generator, which extract and compile data and statistics from the system's database tables. DoE confirmed that the above tools have been used to create datasets and reports according to the Department's needs. An officer in the grade of Principal has rights to the report builder to edit and build queries, whilst a number of officers in charge of specific examination boards also have access to the report generator albeit with more restrictive rights. The SSRS report generator can produce reports in multiple formats, such as .CSV, .XLS, .PDF and .DOC, to cater for different needs.

4.2 Visitors' Management System

The Visitors' Management System (VMS) is a system which is used to maintain accurate records of all visitors to the Department's offices. The system allows for the recording of both the visitors' details, as well as their reason/s for visit or the service required.

The system ensures that visitors are duly and electronically logged and registered when accessing or leaving the premises.

The VMS has been implemented at the DoE in the second half of 2020. This Office was informed that this system was treated as an extension to MFED's current licence with the same third-party contractor for the VMS at MFED Head Offices in Floriana.

The system is owned by IMU-MFED, whilst the DoE is an additional user of this system. Meanwhile, the NAO was informed that the DoE is the data owner in respect of all data collected from within their offices only.

The relevant equipment/hardware and the system/software licences were procured, through IMU-MFED, from local third-party suppliers, in line with the system installed centrally at MFED Head Office.

Whilst the NAO commends DoE's initiative in investing in and implementing this system from a security aspect, nevertheless, as DoE were in the process of relocating premises during the course of this IT audit, and consequently, the VMS system was temporarily out of use during this period until DoE set up and settle in their new offices.

The VMS is an off-the-shelf software application, part of the Workforce HR suite of programs. The system is cloud-based, and uses Microsoft SQL on Azure.

As the system is hosted on the Microsoft Azure stack, the NAO was informed that backups are being handled by MITA. This setup also means that such backups are always being stored off-site. On the other hand, the DoE stated that such backups are not currently being tested, and no restores have been made from such backups to test and ascertain the reliability of such backups.

Access to the VMS application is controlled and restricted to authorised users/personnel only, via individual user login names, and is password protected. With regards to such passwords, the NAO observed that these are subject to enforced password complexity rules, automatically expire after a specified period of time, and cannot be reused. Additionally, system access is also blocked automatically after a specified number of unsuccessful login attempts.

In the meantime, the NAO was informed that in cases were a user has forgotten their password, the system provides a “Forgot Password” link when logging in, which will automatically trigger the re-issue of a temporary password, which will be sent to the user. Upon successful login to the system with this new temporary password, the user can then change the password from the system.

In terms of account management, maintenance, enhancements, etc., the system is administered by DoE, with support being provided by IMU-MFED.

The NAO was informed that, as at audit date, the seven individuals had user access rights to the VMS software application, including both DoE and IMU-MFED officers. DoE added that none of the third-party supplier’s staff have access to the system.

The NAO noted that the VMS software application had different user levels built into it, according to the duties and roles of the users, including, administrator, organisation creator, approver, and user.

With regard to DoE users of the system whose employment has been terminated, the Department claimed that such users and their login credentials are removed from the system by the administrator, and access to this system will no longer be possible.

Furthermore, DoE clarified that users on maternity leave, prolonged leave or career break, would have their login access to this system disabled for the period in question. However, the Department stated that as at audit date, they had not yet encountered any such occasion/instance.

This Office was pleased to note that the VMS software application does not allow the deletion of any records/data, by any of the system’s users. Moreover, in terms of audit trails, this Office was informed that the system has a built-in audit log. In this regard, IMU-MFED added that anonymisation of data occurs after a specific period of time, so as to protect the privacy of individuals.

DoE reported that any initial bugs that were present in the VMS were now resolved. In the meantime, DoE also indicated that no enhancements to this system have been required yet, and in this regard, this Office acknowledges that the system had only been in use for a few months at the time of the audit.

In parallel with this, the Department commented that the process, which is automated by the VMS, is not a complex one, implying that the need for a business process reengineering exercise is low at this point in time.

Nevertheless, this Office observed that the provision of maintenance and support of the VMS and ancillary services is not yet governed and regulated by a service level agreement between the third-party supplier and the DoE. Instead, as at audit date, the auditee and the third-party supplier are only bound by and subject to the terms of the initial quotation for licencing this software application. This implies that the latter was not yet bound with specific response times with regard to provision of support concerning potential bug fixes and upgrades.

The audit team was informed that programming manuals for this software application are not available. On the other hand, this Office was pleased to note that user manuals were provided by the developer and are available online[19].

The audit team also learned that with regard to training, new DoE users of this software application are provided with on-the-job training.

In terms of reporting functionality, the audit team was informed that the system also has a report generator. In this regard, DoE stated that reports from this system can be issued upon request, and confirmed that this report generator meets the requirements of the Department.

4.3 DoE Website

The official website of the DoE is https://myexams.gov.mt/. The website was launched in 2019 replacing the Department's previous website.

The website was created and developed by a local third-party contractor, who is also responsible for hosting this website. The NAO was informed that the Department opted for private hosting, for the website, for technical reasons, in line with directions of IMU-MFED.

DoE is the owner of the website and is responsible for all content management. Internal backend access is restricted to a limited number of authorised users only, and is password protected. Meanwhile, the third-party developer of the website is responsible for the provision of technical support, under the supervision of IMU-MFED.

Following enquires made by the audit team, DoE claimed that the website is updated regularly, at least once a month, or when it is required, adding that this is in line with the Department's scope, which is to keep the public and their clients updated with the most recent information concerning examinations regulations, dates and other pertinent information.

[19] User manuals available at https://workforce.com.mt/docs/

Upon reviewing the website, the NAO immediately observed that the website is optimised for both mobile as well as desktop devices, is relatively intuitive and user friendly, and is also bi-lingual offering a choice of Maltese or English languages.

The website provides ample information, with specific pages about the Department and the services it offers to clients/candidates, the individual DoE sections and their functions (including detailed 'frequently asked questions'), the Examination Boards with whom the Department co-operates and whose examinations are offered, details of the venues where DoE holds examinations, and the DoE's contact details, as well as a number of quick links. In addition, a specific page notifies of current and up-to-date applications for upcoming examinations and related posts.

Furthermore, the DoE's website also provides a specific page allowing local e-ID holders to login and access additional facilities. The DoE stated that when examinations sessions are available, potential clients and candidates may register for most of their examinations directly online, as well as pay for these examinations also online by credit card. The NAO noted that when no examination sessions are available, very little information is provided to the end user on the related web page.

The NAO positively observed that the website landing page also includes a link to the DoE Privacy Policy, Data Protection Policy and the web Accessibility Statement.

During this review, the NAO also observed that the DoE's old website, https://exams.gov.mt/, whilst still up and running, provides ample notifications and links to the DoE's new website, on almost every page. DoE eventually clarified that, as at audit date, the old website is still active since the application system for the EMS is still linked to this website, and when one applies through the new website, a 'workaround' was enacted whereby the new website connects to the old one.

Finally, in terms of documentation, the audit team gathered that whilst a detailed initial project proposal by the third-party contractor, including a quotation with a breakdown of costs with provision of support, as well as an invoice for the design and implementation of the website, were made available, however, a copy of the service level agreement was not provided to this Office.

4.4 Social Media

The audit team gathered, during the course of this IT audit, that DoE makes good use of modern communications technology platforms[20] and tools to facilitate its work (including online meetings, general communication, messaging, document sharing, etc.) to connect members of staff, and with examination boards and other entities, particularly during the COVID-19 pandemic. However, the NAO observed that currently, DoE does not make use of any of the popular social media and networking platforms[21] to enhance its online presence and extend its reach to its clients and the general public. Furthermore, at the time of this audit, the DoE did not have any plans to utilise such social networking platforms in the near future.

[20] Modern communications technology platforms such as Microsoft Teams, Zoom and WhatsApp, amongst others.

[21] Popular social media and networking platforms such as Twitter and Facebook, amongst others.

4.5 Observations, Conclusions and Recommendations

Examinations Management System

Referring to backups, the NAO advises that the DoE and IMU-MFED should ensure that regular backups are being taken, and should ascertain that periodic restores are also being performed and signed-off, to assure dependability and availability in case of requirement for emergency.

In terms of user accounts and access, the Office recommends that logins of DoE employees on prolonged leave, career break or maternity leave should be temporarily disabled from the system during the period of absence.

With regard to a business process review, the NAO opines that such an exercise would be beneficial to the Department, particularly if moving towards an updated/upgraded or new system. In this manner, processes or procedures may be introduced or modified in this system, in line with the DoE's business process, thereby increasing efficiency.

Furthermore, the NAO also reiterates that the DoE should ensure that a signed copy of the service level agreement with the third-party contractor is always readily available, and periodically review such agreements with IMU-MFED to ensure full compliance by the third-party contractor with all clauses. Furthermore, the DoE should consider the inclusion of relevant penalty clauses in these contracts.

Additionally, the NAO also suggests that system programming manuals should be made available, and DoE and IMU-MFED should ensure that these are kept relevant by being kept current and up-to-date.

Visitors' Management System

The DoE should ascertain that the data being collected is not excessive, and is in line with GDPR provisions.

With regard to backups, this Office recommends that the IMU-MFED and DoE should ascertain that regular backups are being taken, as well as verify that that periodic restores are also being carried out and signed-off, to guarantee dependability and availability in case of requirement for emergency.

In terms of the provision of maintenance and support of the system, the NAO strongly recommends that this should be covered by a service level agreement between the third-party supplier and IMU-MFED/DoE, to ensure that any current and applicable terms and agreements are formalised into a legal document. This should specify service level/performance indicators, and document relevant procedures/processes. Any further enhancements to the system should similarly be covered by a specific agreement/contract.

Moreover, this Office also recommends that, if possible, the system's source code and related software development documentation should be made available, and DoE and IMU-MFED should ascertain that these are kept relevant by being kept current and up-to-date.

IT Software Applications - General

Given the ICT investments made by MFED, the NAO suggests that DoE management discusses and liaises with IMU-MFED to get a thorough overview of the existing pool of MFED's education IT systems, which may hold valuable data of relevance to the further automation and facilitation of DoE business process and functions. The DoE management may then consider obtaining access to such data or introducing such systems at the Department as required, with the aim of increasing efficiency.

DoE Website

Referring to the current website setup and hosting (privately with third-party, not with MITA), this Office acknowledges that such a setup may provide a higher level of flexibility to DoE and IMU-MFED. However, the NAO opines that this situation also implies that IMU-MFED and DoE must take all the necessary steps to ascertain continued full compliance with all GMICT web related policies.

With regards to the DoE website itself, the audit team observed that whilst the examination venues in use by the Department are listed on a specific page on the website, however, the full address and general direction to get there are absent. The NAO recommends the inclusion of the address and a link to the exact location on a map.

Moreover, given that the new DoE website has been online since 2019, the NAO recommends that DoE addresses any current online application links to the old website in order to remove dependency on this old website. Furthermore, the Department should consider the possibility of removing access to the old website completely, whilst ensuring that all external links to the DoE website direct users to the new URL.

In terms of the provision of maintenance and support of the website, the Office strongly recommends that this should be covered by a service level agreement between the third-party contractor and IMU-MFED/DoE. In this regard, any current and applicable terms and agreements should be formalised into a legal document, and not just subject to the original project proposal and quotation. This should specify service level/performance indicators, and document relevant procedures/processes. Any further enhancements to the website should also be covered by a specific agreement/contract.

Social Media

This Office strongly recommends that the DoE considers enhancing its reach and accessibility to its clients and the community, through the use of social media platforms popular for interacting with the general public.

Chapter 5 | Information Security and IT Risk Management

This chapter takes a look at information security controls and IT security measures adopted by DoE to maintain integrity, confidentiality and availability of data. Furthermore, this chapter also looks at the management of IT risks within DoE to identify, assess and prioritise potential risks, so as to draw up related recommendations to mitigate or reduce such risks.

5.1 Anti-Virus and Malware

The control and prevention of spread of malware is managed by IMU-MFED through MITA. Anti-virus definitions and malware threat protection updates are pushed automatically by MITA to all workstations that are joined to MITA's Corporate Domain, thus safeguarding the DoE's IT assets which are covered by the related anti-virus and malware protection software.

5.2 Information Classification, Data Retention and Protection

The NAO notes that the DoE does not have a specific Information Classification Policy notwithstanding the volume and type of data being held/retained by the Department, which implies that an internal process where this data is being informally classified is probably already in place. In this regard, this was indirectly affirmed by DoE, which acknowledged that the Department does in fact have personal data which is considered 'confidential'.

Furthermore, DoE stated that access to examination papers, including questions, answers and correspondence (in electronic format), prior to the examination sessions, is governed by the regulations related to the specific examination board in question.

With regards to Data Retention and Data Protection, DoE stated that the Department has drawn up policies for both areas. Copies of both documents were made available to this Office for review.

The NAO observed that the Data Retention Policy, was endorsed and approved by the National Archivist of Malta in 2018, and is to be reviewed at least every five years. It was explained that this policy, classifies the type of data and information, whether in soft form or hard/printed form, that is kept by the Department, as well as its period of retention. The NAO notes that the policy guarantees that the DoE's records are properly appraised, and that records of enduring historical value will in due time be transferred to the National Archives for permanent preservation.

On the other hand, the NAO noted that the Data Protection Policy is set to comply with the Data Protection Act (Chapter 440) and states that data is held and processed in terms of the relevant sections of the Education Act (Chapter 327), and related local and overseas examining bodies, in order for the Department to fulfil its functions, whilst stating why it needs to process its clients' data. The policy also indicates the entities who may be the recipients of this data, and outlines its clients' various rights, including the procedure for dealing with a request by a data subject to access personal data held, and how the DoE Data Controller may be contacted. However, the NAO was not provided with a copy of the policy which was dated and endorsed by DoE management.

In this regard, this Office commends these initiatives to properly assess and review the DoE's data/documentation, particularly in view of the nature of such information which is being collected by the Registrar of Examinations, whilst safeguarding its clients' data and rights.

5.3 Physical Access Controls

During the on-site review at DoE premises carried out during audit, the audit team observed the physical access security controls/measures that were in place on site at DoE main building in Floriana. In this regard, the DoE indicated that a closed-circuit television (CCTV) (video surveillance) system, and a visitors' management system have been installed. In addition to the above, the audit team also observed physical access controls specific to the office housing the network cabinet, as highlighted earlier on in Section 3.1.6.

5.3.1 Visitors' Policy

During the course of this audit, the NAO also examined additional controls in place related to logs of visitors at DoE. In this regard, it was established that there is no formally documented visitors' policy in place at DoE, with the Department claiming that they are moving in a direction where over time, various manual process are converted into online applications, and its clients (the general public) are attended to and supported online, via such IT software applications, emails, etc., thereby reducing drastically the need for clients to physically visit the offices to be served.

During the on-site visits, the audit team also observed that a visitors' logbook/register was being maintained. Furthermore, the audit team learned that DoE has recently invested in a Visitors' Management system (VMS), which ensures that visiting clients present on site at DoE offices are registered appropriately. A more in depth look and further details on this software application were given in Chapter 4 of this report.

5.3.2 Video Surveillance System

The video surveillance system, covered both the ground and first floor, including the main entrance of the building, at the DoE offices in Floriana, whilst only the common areas, such as corridors, open areas, access to strong room, etc., were covered by the CCTV system, in line with general data protection guidelines. In total, the NAO observed that there were seven cameras installed on site[22].

Additionally, DoE specified that that some of these cameras, notably those covering the main entrance and shared common areas, were shared by DoE with the Directorate for Learning and Assessment Programmes (Curriculum Department), housed on the second floor of the same premises. Nonetheless, DoE explained that their initial intentions when deciding to invest in a CCTV system, which was installed in 2019-2020, were to ensure that the DoE strong room is always kept secure and safe.

The NAO was informed that CCTV system was set up so as to retain (record) footage for a period of 20 days, following which this is automatically overwritten. The footage was stored electronically and could be accessed via login and password by the Director DoE himself. Whenever the footage needs to be viewed, another officer will be appointed by the former to act as the Director's delegate. DoE also remarked that no written records were maintained in cases where access to the footage was required, although to date, there were no instances where access to such footage was required.

5.4 Fire Prevention and Fire Suppression systems

The NAO was informed that the smoke/fire detection system installed at the DoE offices in Floriana[23], automatically alerts the DoE's senior management officials, as well as the Malta Police Force and the Civil Protection Department, when such a risk arises. The DoE stated that it had invested in this system in 2020.

The DoE clarified that this system is also shared by DoE with the Directorate for Learning and Assessment Programmes (Curriculum Department), housed on the second floor of the same premises.

The NAO was also informed that the above-mentioned system is complemented with fire extinguishers which are installed in proximity of every room, in all levels of the building, housing the DoE offices in Floriana. In this case, it was noted that this fire suppression equipment is not shared with the Curriculum Department located on the second floor.

The DoE indicated that these fire extinguishers are duly inspected and serviced regularly by the respective third-party service provider, with the last inspection having been carried out at the beginning of 2021, and the next one scheduled at one year's interval for early 2022.

It was also observed that this equipment is easily accessible by all members of staff, and the NAO was pleased to note that three employees have been given specific training for fire control management and personnel evacuation. This training was provided on site, when the system was initially installed.

[22] These cameras were eventually removed from this site once the DoE vacated the premises. No additional information concerning CCTV coverage at the new site/offices was available during audit testing.

[23] Pursuant to DoE vacating these offices and eventually relocating, the smoke/fire detection system was disconnected/removed and then reinstalled at the St. Elmo Examinations Centre, Valletta. No additional information concerning the setting up of such a similar system at the new site/offices was available during audit testing.

5.5 Business Continuity and Disaster Recovery

Following enquiries made by this Office, it transpired that the DoE has neither conducted a business impact analysis nor a risk assessment exercise as at audit date. DoE does not have a Business Continuity Plan (BCP) or a Disaster Recovery Plan (DRP). In this regard, DoE reiterated that such exercises fall under the remit of IMU-MFED and MITA.

DoE also claimed that there were no particular incidents of non-availability of key IT systems which might have impacted its overall operations in the past. Nonetheless, as highlighted earlier on in this report, the NAO in fact observed a number of issues that cropped up with DoE's main application (the EMS) during the course of this audit, which partly impacted DoE's operations.

Furthermore, DoE remarked that, at least for local public examinations, most of the processes, such as registrations, etc., were carried out manually, and only through time were these converted into online applications. However, DoE stated that this conversion/switch from manual to online applications/services was done incrementally over the years, but did not provide an approximate timeline for this process, whilst asserting that virtually all examination applications/services were online by 2020.

Moreover, DoE indicated that in the event of a total IT systems failure, the Department will revert to manual processes, so as to temporarily maintain operational functionality for its business processes and meet its timelines and deadlines concerning various examinations held. DoE also stated that, even though at present it does not have any specific standard operating procedures applicable in case of a total IT systems collapse, however, written standard operating procedures do exist for both manual and online DoE applications. In this regard, copies of the relevant standard operating procedures applicable for Secondary Education Certificate, Intermediate level, and Advanced level examinations, which are the principal uses of the EMS software application, were provided to the NAO as evidence.

Finally, the NAO also confirmed that DoE does not have any alternative site from where it could resume its key operations in the event of a disaster.

5.6 IT Security Awareness Training

In response to enquiries concerning IT security awareness training provided to DoE's employees, such as that relating to the smart/safe use of internet, email, etc., the Department referred to MITA's information/security notification emails regularly pushed to all public service and public sector employees on these topics, adding that, whenever there is an issue specific or relevant to DoE and its staff, senior management raises the matter with DoE employees, either through a memo or an email, as necessary.

5.7 Observations, Conclusions and Recommendations

Information Classification, Data Retention and Protection

In view of the volume of data being handled by the Department, the NAO recommends that DoE management should ensure that the internal process/es where this data is being classified, is formalised by drafting an official policy governing the classification of information. This should facilitate the process of classifying data being processed by the DoE (ex. confidential, restricted, sensitive, personal etc.) and would be applicable in scenarios such as access to examination papers, including questions and answers (in electronic format), before the examination sessions, etc.

Furthermore, the NAO recommends that DoE management should always ascertain that signed and dated copies of all policies are always at hand.

Physical Access Controls

Given that the DoE was preparing to relocate its offices to a new site subsequent to audit testing, this Office recommends that all efforts must be made by the Department to ensure that as a minimum, the same level of physical access controls are present in the new site.

Furthermore, the NAO recommends that DoE management drafts an official policy governing visitors' access to DoE offices, outlining procedures to be adopted such as, specifying any restricted areas, logging in and out of all visitors, and situations where visitors would need to be accompanied by members of staff.

With respect to the installation of the video surveillance system at the new site, the NAO recommends that the DoE ensures that the same level of controls relating to the storage, retention and access to the CCTV footage, are maintained when settled at the new offices.

Fire Prevention and Fire Suppression systems

The NAO recommends that DoE ensures that adequate fire prevention and suppression systems are installed at the new office location. Furthermore, the Department is to ascertain that these systems are adequately and regularly inspected and serviced, whilst the necessary training is to be provided to selected DoE members of staff.

Business Continuity and Disaster Recovery

The NAO recommends that the DoE drafts a BCP and DRP which would include the possibility of using an alternative site (such as an office within an MFED building) to access DoE systems, which are hosted at MITA, should the DoE offices be unavailable due to a disaster. The NAO notes that the need for this BCP and DRP is independent from the existing MITA BCP and DRP as this would only cover the continuity of MITA services, whereas a DoE BCP and DRP ensure the continuity of DoE business operations until normal operations are restored.

IT Security Awareness Training

The NAO recommends that the DoE management organises IT security awareness training sessions for its personnel on a regular basis (as a minimum, once a year) so as to increase awareness amongst its employees on potential and current IT security risks (such as best practices to protect against current ransomware attacks) which could potentially affect the Department, its assets, and its business continuity.

In this regard, DOE management could liaise with the institute for the Public Service (IPS) to apply for security awareness training sessions which are on offer from time to time.

Chapter 6 | Management Comments

The final chapter of this report presents the comments given by DoE senior management following review and discussion of this report.

6.1 DoE Management Comments

DoE senior management provided the following comment on this IT audit report:

"The report gives a thorough evaluation of IT within the Department of Examinations, and acknowledges the progress made whilst also giving a number of important recommendations. It is, however, to be noted that as with all Government Departments, the Department of Examinations is part of the Ministry for Education and of the Public Service in general. As such a number of functions are dealt with either through IMU-MFED or through MITA as per Government policy. In these cases, recommendations may not always be pursued as this could not only be beyond the direct control of the Department of Examinations, but also contrary to general policy within the Public Service regarding IT systems. The report accurately reflects the Department's commitment to further enhance the service provided to the Public and to improve its digital capacities."

Furthermore, DoE senior management also made the following additional comments/remarks on this report:

- With regards to the drafting of a specific DoE IT strategy and annual IT budget, in line with those at IMU-MFED, DoE stated that "*procurement of IT related material falls within the remit of IMU-MFED…*"

- With regards to signed copies of service level agreements, the DoE stated that they "*have SLAs regarding the VMS and the DoE website*" and that "*such agreements are made and maintained through IMU…DoE is only given a copy*". Meanwhile, a signed copy of the EMS service level agreement was made available to the NAO at the end of this IT audit.

- Further to the above, DoE stated that the inclusion of the relevant penalty clauses within these contracts "*would need to be discussed and negotiated through IMU*".

- Referring to the possibility of engaging a full time IT officer, DoE stated that "*when this matter was discussed with IMU…lack of human resources*" was indicated.

- In reference to the secure wiping of data before disposing or transferring IT equipment, DoE added that as they "*do not have administrator status…wiping of devices must be done by IMU*".

- In reference to the recommendations made concerning the network cabinet to be utilised at the DoE's new offices, DoE noted that this "*is going to be as recommended*".

- Referring to the possibility of extending outside working hours, the support service offered through the DoE's generic email account, DoE stated that "*current human resources do not allow for this*".

- With regards to the drafting of a standard operating procedure to cover confidential access to audit logs of DoE systems, DoE stated that "*audit logs…may be requested with the Director's approval*" whilst outlining that audit logs for the EMS application "*…would be made available by making a request to IMU and supplier*".

- Similarly, regarding the drafting of a suitable policy governing the use of personal portable and mobile devices within the Department's offices, the Department stated that "*…this is covered by MITA/IMU policies, to which we adhere*".

- In reference to the upgrade and revamp to the EMS application, DoE commented that "*this is currently ongoing and is in the process to be concluded in the near future. It will comprise solutions to other issues not envisaged at the time…The migration process is ongoing because it now includes workarounds for connection to the Government Payment Gateway where a better audit trail is also being implemented...*". DoE also remarked that "*…However, it is noted that at pilot project stage, the reforms in MATSEC examinations did not require specific upgrades*".

- Furthermore, the DoE added that when the above-mentioned migration is completed, the link to the old website will no longer be required.

- With reference to the VMS application, DoE clarified that "*VMS will no longer be used in our new premises…since access of visitors to our Department will now be controlled by the main Reception...*".

- With regards to the availability of system programming manuals for DoE's applications, the DoE stated that "*…it is possible to tell the suppliers to make these available*".

- In reference to the utilisation or access to MFED's education IT systems, DoE stated that "*while this may be discussed…with IMU-MFED, …we do not envisage much scope for this as much of the data is sensitive and personal and covered by data protection regulations*".

- Referring to the inclusion of the address and a link to the exact location on a map in relation to examination venues listed on the DoE website, the DoE commented that "*this can be done*".

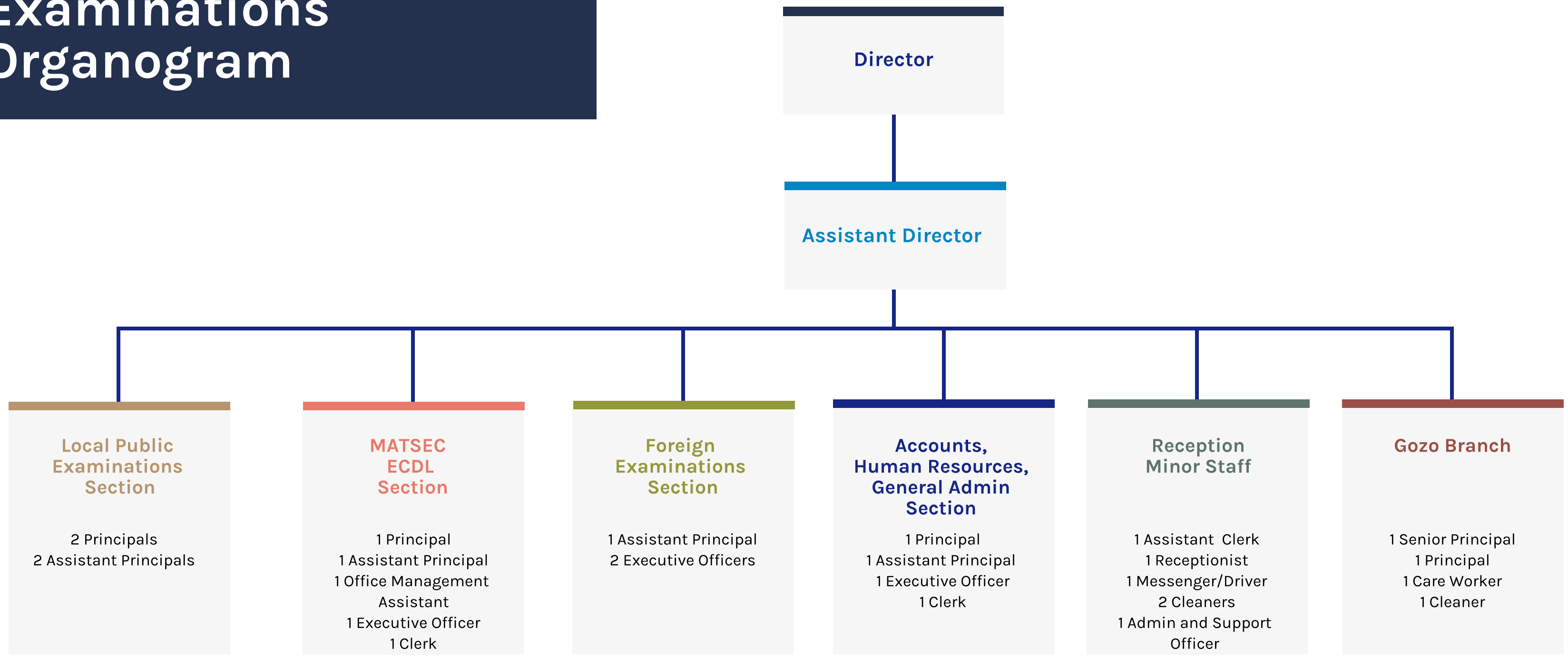
- With reference to the utilisation of social networking platforms to increase interaction with the general public, the DoE stated that "*current human resources do not allow for this*".

- Referring to DoE's relocation of offices to a new site and the related security controls, the Department commented that "*these are already in place"* and that *"access controls are also in place*". DoE also remarked that "*CCTV footage is automatically deleted after…*" a specific period and that the "*fire detection system lies within the responsibility of the owner… not DoE anymore".* Furthermore, DoE also clarified that the new building "*includes fire detection in all rooms, but not fire suppression. A number of fire extinguishers are present*".

- With regards to the drafting of a BCP and the DRP, DoE stated that "*access to operations, including VPN, are all in place*" and that "*all departmental operations – in such circumstances – can all be carried out remotely, even from home".* Meanwhile, DoE also noted that *"all applications are now online*".

Appendix

Department of Examinations Organogram



Director

Assistant Director

Local Public Examinations Section

2 Principals
2 Assistant Principals

MATSEC ECDL Section

1 Principal
1 Assistant Principal
1 Office Management Assistant
1 Executive Officer
1 Clerk

Foreign Examinations Section

1 Assistant Principal
2 Executive Officers

Accounts, Human Resources, General Admin Section

1 Principal
1 Assistant Principal
1 Executive Officer
1 Clerk

Reception Minor Staff

1 Assistant Clerk
1 Receptionist
1 Messenger/Driver
2 Cleaners
1 Admin and Support Officer

Gozo Branch

1 Senior Principal
1 Principal
1 Care Worker
1 Cleaner

2020-2021 (to date) Reports issued by the NAO

NAO Annual Report and Financial Statements

May 2021	National Audit Office Annual Report and Financial Statements 2020

NAO Audit Reports

October 2020	Follow-up Reports by the National Audit Office 2020 Volume II
November 2020	Information Technology Audit: Planning Authority
November 2020	Performance Audit: An analysis of Malta Medicines Authority recruitment process
November 2020	Information Technology Audit: Malta Industrial Parks Ltd
November 2020	Report by the Auditor General on the Workings of Local Government for the year 2019
December 2020	Report by the Auditor General on the Public Accounts 2019
December 2020	A review of implementation of Sustainable Development Goal 1 - Malta's efforts at alleviating poverty
January 2021	Performance Audit: Is LESA suitably geared to perform its traffic enforcement function adequately?
February 2021	Performance Audit: The effectiveness of plastic waste management in Malta
April 2021	The contract awarded to the JCL and MHC Consortium by the St Vincent de Paul Residence for the management of four residential blocks through a negotiated procedure
May 2021	Performance Audit: Preliminary review: NAO's role in reviewing Government's measures relating to the COVID-19 pandemic
June 2021	Follow-up Reports by the National Audit Office 2021 Volume I
July 2021	Performance Audit: Fulfilling obligations in relation to asylum seekers