National Audit Office
MALTA

Information Technology Audit

Mater Dei Hospital

Report by the Auditor General

May 2016

SPTAR MATER DEI

Information Technology Audit

Mater Dei Hospital

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AMS	Asset Management System
BCP	Business Continuity Plan
BUPA	British United Provident Association
Cath Lab	Catheterisation Laboratory
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CIMU	Central Information Management Unit
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
CPAS	Clinical Patient Administration System
CPSU	Central Processing and Supplies Unit
CT	Computed Tomography
CTMS	Central Theatre Management System
CTSO	Centralised Theatre System Office
CVIS	Cardiovascular Information System
DCU	Day Care Unit
DICOM	Digital Imaging and Communications in Medicine
DMU	Data Management Unit
DoS	Denial of Service
DRP	Disaster Recovery Plan
ECG	Electrocardiogram
ECS	Electronic Case Summary
EESI	Electronic Exchange of Social Security Information
e-mail	Electronic Mail
ENT	Ear, Nose and Throat
eRFS	Electronic Request for Service
ETL	Extract, Transform and Load
EU	European Union
FMS	Foundation for Medical Services
GGH	Gozo General Hospital
GMICT	Government of Malta Information and Communication Technology
GU	Genitourinary
HAA	Hospital Activity Analysis
HL7	Health Level Seven
ICD	International Classification of Diseases
iCM	iSoft Clinical Manager
ICT	Information and Communications Technology
IHE	Integrating the Healthcare Enterprise
IM&T	Information Management and Technology
IMU	Information Management Unit
IT	Information Technology
ITIL	Information Technology Infrastructure Library

ITSM	Information Technology Service Management
ITT	Invitation to Tender
ITU	Intensive Therapy Unit
LAN	Local Area Network
LIS	Laboratory Information System
LPO	Local Purchase Order
MAGNET	Malta Government Network
MCH	Mount Carmel Hospital
MDH	Mater Dei Hospital
MEH	Ministry for Energy and Health
MITA	Malta Information Technology Agency
MM&L	Materials, Management and Logistics
MOP	Medical Outpatients
MRI	Magnetic Resonance Imaging
NAO	National Audit Office
NAS	Network Attached Storage
OA	Office Automation
ORS	Online Requisition System
OSR	Online Surgical Register
PACS	Picture Archiving and Communication System
PAHRO	Public Administration Human Resources Office
PAS	Patient Administration System
PC	Personal Computer
PET	Positron Emission Tomography
PID	Personal Identification
POYC	Pharmacy Of Your Choice
RFID	Radio Frequency Identification
RIS	Radiology Information System
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAMOC	Sir Anthony Mamo Oncology Centre
SHE	Segregated Hosted Environment
SLA	Service Level Agreement
SLH	St. Luke's Hospital
SOP	Standard Operating Procedure
SPBH	Sir Paul Boffa Hospital
SVPR	St. Vincent de Paule Residence
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WHO	World Health Organisation

Executive Summary

Executive Summary

Background

The National Audit Office (NAO) carried out an Information Technology (IT) audit within Mater Dei Hospital (MDH). This audit sought to examine MDH's IT operations and IT-enabled investments to ensure that IT is successful in delivering the business requirements.

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

Key Findings and Recommendations

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

a. The NAO observed that in the majority of the IT software applications reviewed, only one ICT Application officer was supporting a particular system. On the other hand, the Networks team within the Information Management and Technology (IM&T) unit was manned by only two officials who were involved in the planning of the migration of a number of IT software applications to MITA's Segregated Hosted Environment (SHE), monitoring of the backup processes and the management of the MDH server room infrastructure amongst others. Furthermore, at the time of the IT audit, these two officials resigned from MDH and as a temporary measure, some ICT Application officers were assigned the duties of the IM&T Networks team.

The NAO recommends that in cases where only one individual is supporting a critical software application within MDH, additional resources are allocated to remove the dependency from these individuals. Moreover, sufficient human resources should also be engaged to fill in the posts vacated within the Networks team.

b. The NAO was informed that the Medical Records department is running out of space and will soon be finding it difficult to stack more patients' files. In this regard, the NAO was informed that the Medical Records department, together with the Director Health Informatics and the MEH are looking for options to provide a simpler way of storing patients' health information, including digitisation.

The NAO therefore recommends that MDH analyses the options being considered without delay, whereby patient's health information may be scanned and saved electronically thus reducing the volume of the physical files and the related storage space required.

c. The NAO observed that an ICT Support officer took the initiative to create user manuals and pamphlets for end users attending to training and which can also be downloaded from the IT Trainers portal. It was also noted that the IT Trainers portal was designed and is being maintained by the same ICT Support officer.

The NAO recommends that the IT Training section should consider offering e-Learning or m-Learning facilities to the end users according to their job function within MDH, or other sites within the Ministry for Energy and Health (MEH) through the IT Trainers portal.

d. The NAO was informed that the IM&T unit had drafted an IT strategy for MDH, in line with the Ministry's IT strategy. At the time of the IT audit, this IT strategy still needed to be finalised and approved by the Ministry.

The NAO recommends that the IT strategy is given its due importance, and is finalised and approved by the Ministry as soon as possible.

e. The NAO observed that the IT Technical Support team does not securely wipe hard disks whenever a Personal Computer (PC) or laptop is transferred to a different user or is disposed of.

The NAO recommends that the IT Technical Support team adopts the Government of Malta Information and Communication Technology (GMICT) Desktop Services Procedure (GMICT R 0084:2009)[1] in terms of PCs or laptop disposal and data wiping, and ensures that data on the equipment being disposed of could not be retrieved by any third party.

[1] https://www.mita.gov.mt/MediaCenter/PDFs/1_GMICT_R_0084_Desktop_Services.pdf

The IT audit reviewed 14 software applications used within MDH (Chapter 3 refers) in terms of ease-of-use, security controls, account management and hosting services. The main findings and corresponding recommendations are listed below:

a. The Access Dimensions application has a Microsoft SQL database with two instances, whereby one of the instances resides on a dedicated Microsoft Windows 2000 server. MDH is aware that the Microsoft Windows 2000 server is obsolete and no longer supported by Microsoft, and furthermore the server hardware is also quite old and thus has its limitations.

   The NAO is of the opinion that the above-mentioned server is decommissioned and the SQL database is migrated on a virtual environment and hosted at MITA's SHE.

b. The NAO was verbally informed that there were instances in the past whereby the Centricity Radiology Information System (RIS) application was installed on workstations without the ICT Manager's consent when the latter was unavailable. This contributed to the further saturation of user licenses and the hardware and software inventory not being updated.

   In this regard, the NAO is of the opinion that RIS installations should always be approved by the ICT Manager to ensure that such installations are kept under control.

c. Even though the Clinical Patient Administration System (CPAS) application was launched in 2013, the old Patient Administration System (PAS) is still running and hosted at MITA's MDH Data Centre. However, the PAS application is not being kept in sync with the current CPAS application, since only some data, such as patient demographics and future appointments, was migrated from the previous PAS application.

   The NAO is of the opinion that all the relevant data is completely extracted from the PAS application and presented in a readable format.

d. At the time of the IT audit, the NAO observed that users from different departments raised a number of issues, when updating the '*Patient Interface*' module on CPAS. There are instances whereby the '*Age*' field is blank and not calculated automatically even though the patient's date of birth was inputted correctly. This may lead to a situation where the user cannot determine at a glance whether the patient is under age and should be accompanied by an adult.

   Taking into consideration that the CPAS application provides patient demographics to a number of critical applications within MDH, the NAO recommends that MDH should continuously emphasise on the importance of updating the patient demographics and to provide the necessary enhancements to the '*Patient Interface*' on the CPAS application.

e. The NAO observed that certain users are having difficulties finding available slots to be allocated in a particular clinic, when setting up an appointment. This is due to the fact that some clinics are overloaded with patient appointments especially at the outpatient's department. If a Consultant requests that a particular patient is admitted to MDH for a follow-up on a particular date but all

the available slots on CPAS are booked, the Clinical Nurse assisting the respective Consultant has to phone the CPAS team to add a new slot for that particular clinic.

In view of this, the NAO recommends that MDH should look into this matter and evaluate whether elevated privileges can be assigned to specific users so that they can allocate new slots to a particular clinic when applicable.

f. The NAO was informed that the audit trail functionality on the MDH Dakar application was disabled as it was generating too many logs, which affected the performance of the system.

The NAO recommends that key stakeholders within MDH together with the local third party supplier should review the current MDH Dakar application and server specifications, and come up with a solution to re-enable the audit trail functionality without impacting the performance of the system.

g. The NAO noted that the MDH Dakar application cannot process pro-rata calculations, affecting any type of '*variable*' allowance or deduction. Consequently, these pro-rata adjustments have to be calculated manually by the payroll officers, before inputting the amount due, and applying the relevant code/s in the Dakar Payroll system.

In addition, when a payroll adjustment is required after examining the attendance records, there may be instances whereby the officer has to manually work out the adjustment and only input the final result, together with the relevant code, in Dakar for further processing. Similarly, when examining overtime sheets to establish the '*other*' overtime due, the officer has to manually work out the applicable overtime rate, apply this rate to calculate the actual amount of overtime due, and then finally input the monetary amount in Dakar for further processing.

At the time of the IT audit, the MDH Dakar application catered primarily for approximately 4,400 employees and has around 1,700 roster variations of which approximately 800 were currently active. Moreover, due to the lack of any electronic attendance recording system at MDH, the attendance is recorded manually in around 700 different timesheets.

The NAO also noted that when inputting an amount intended for a '*negative*' payroll adjustment, along with the applicable code for a deduction, the system does not process the amount as a deduction by default, and the user has to remember to key in the negative sign ('–') in front of the amount.

Additionally, when an unrealistic amount of substantial value has been inputted, the software application does not prompt or warn the user to ascertain that this is correct. Such an error can easily result through an oversight, such as forgetting or misplacing the decimal symbol ('.'), or pressing the same number key twice or more.

Furthermore, when a payroll adjustment or amendment to a roster has been manually inputted, the software application does not prompt the user to update, save and lock the data. This would ensure that this is not modified by other users, and that the changes applied are taken into

consideration and correctly processed by the system. In fact, the application depends on the user to remember to tick ('✓') the '*manual change*' box, which by default is blank, and press the '*lock/update all*' button, once the changes have been inputted.

Following the issues highlighted above, the NAO is concerned with the high dependency on manual input on the MDH Dakar application, making it prone to human error. To mitigate these risks, the NAO recommends that MDH's management reviews its payroll business process holistically, and assess the possibility of enhancing the current system. The aim is to automate the process as much as possible, as well as to minimise the dependency on the end users.

h. The NAO observed that the myHealth application does not offer the functionality for parents or guardians to view medical records of children less than 14 years of age under their care. However, individuals over 14 years of age or those who are already in possession of a new e-ID card may submit a request for an e-ID account to be able to view their medical records.

The NAO recommends that the Health authorities explore ways how parents or guardians can apply and obtain access to medical records of children under their care. In this regard, if approval is given, the parent or guardian could then select the Doctor or Paediatrician of their choice.

i. Most of the IT systems reviewed during the course of the IT audit are integrated with the CPAS application. However, the NAO observed that a few other software applications, such as the Day Care Unit (DCU) application, are not integrated with CPAS to retrieve patient demographics.

The NAO recommends that such software applications are integrated with the CPAS application, thus avoiding any inconsistencies in patient's demographics and eliminating the duplication of work in maintaining such data on both CPAS and the IT systems in use within MDH.

Furthermore, MDH should develop an IT strategy to promote the further integration of IT software applications within MDH and the possible integration with Government Corporate databases, such as CdB, to retrieve patient demographics.

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

a. MDH holds a considerable amount of personal data, which may be either stored in electronic format or physically kept in a file. The NAO noted that whilst a retention and disposal policy for personal clinical patient data exists with respect to the Medical Records, MDH lacks an internal policy for the secure disposal of any confidential data stored electronically.

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

b. Whenever a user retires or no longer requires access to the system, the NAO was informed that the user account is disabled only if the ICT Application officer is informed through the Government e-mail. A similar procedure is applied for users who are on prolonged leave, career break or maternity leave, whereby the user account is disabled until the user returns to work.

   In this regard, the NAO recommends that an internal policy is drafted, which clearly indicates that whenever a user retires or no longer requires access to the system, the IM&T unit are informed, and the respective user accounts are disabled or deleted accordingly.

c. The NAO observed that whilst blank passwords are not allowed, most of the IT systems selected for the purpose of this IT audit including Access Dimensions, CPAS, DCU and Dakar amongst others, do not adhere to password management best practices. In this regard, these IT systems do not offer sufficient password security controls, in terms of password complexity, password expiry, and password history, nor do they force the user to change the password upon first logon.

   The NAO is of the opinion that IT systems, which do not offer sufficient password security controls, should be enhanced and adhere to the GMICT Password policy[2]. Furthermore, the NAO recommends that Information Security Awareness guidelines and training should be ongoing, whereby officials within MDH are provided with regular updates to foster security awareness and compliance with security policies and procedures.

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

a. Whilst reviewing the software applications selected for the purpose of this IT audit, the NAO observed that certain users phone the ICT Application officers directly whenever they require assistance. In this scenario, since these calls are not being logged through the proper channels, the IM&T unit cannot quantify exactly the number of incident requests that were serviced periodically, and whether the incidents are repetitive or correlated to identify and solve the root cause of the problem. Furthermore, if all the incident requests are registered through the proper channels, the IM&T unit could substantiate the level of support being provided within MDH, and hence contribute to human resources capacity planning and decision-making.

   The NAO recommends that a memo is issued and circulated within MDH, guiding the users to use the proper channels when logging calls for assistance related to IT systems.

b. The NAO observed that offline mailboxes of personal or generic e-mail accounts are being stored locally on the end users' PC or laptop hard disk.

   Since the end users are not allowed to store offline mailboxes on the MDH shared network drives, the NAO recommends that the IM&T unit should provide guidelines to all the end users within MDH on how to backup and securely store offline mailboxes.

[2] https://mita.gov.mt/en/GMICT/Pages/Security.aspx

c. Whilst reviewing the MDH website in terms of usability and content management, the NAO noted that the MDH website has a number of broken links or missing information. The NAO provided a list of the above-mentioned findings to the Ministry's IMU (Health) to address these issues with the relevant stakeholders. However, at the time of the drafting of this report, the above-mentioned findings still existed.

In this regard, the NAO recommends that these shortcomings should be rectified as early as possible and that Management ensures that the website is updated and made more informative to the general public.

d. At the time of the IT audit, the NAO observed that an official and unofficial MDH Facebook page existed.

Since the general public might not be aware that two different MDH Facebook pages exist, the NAO is of the opinion that the MDH Customer Care department should promote the official MDH Facebook page by providing links on the MDH website and ensure that these pages are continuously updated. Furthermore, the NAO is concerned on the presence of the unofficial MDH Facebook page and is of the opinion that the MDH Customer Care department should also seek advice on the presence of this page as it is misleading the general public in thinking that this is the official MDH Facebook page.

e. The NAO observed that MDH does not have formalised IT Business Continuity and Disaster Recovery plans at the organisational level, covering all the critical IT components within MDH. However, since most of MDH's IT systems are hosted at MITA's Data Centres, MITA has implemented a number of measures to mitigate the risks involved in the event of a disruption or total failure in the IT systems and network infrastructure within MDH.

The NAO is of the opinion that, notwithstanding that most of the IT systems are hosted at MITA's Data Centres and the network infrastructure is monitored and maintained by MITA, MDH should perform a Business Impact Analysis and a Risk Assessment exercise from which a Business Continuity and Disaster Recovery plan can be drafted at the organisational level.

f. The NAO noted that various MDH officials have drafted a number of Standard Operating and Downtime procedures for most of the software applications selected for the purpose of this IT audit, such as CPAS and Centricity RIS and PACS.

Whilst the NAO commends the initiative in drafting these procedures, the NAO recommends that MDH should ensure that every software application should follow the same route and that these documents are continuously updated. Furthermore, every MDH user should be aware of and follow these procedures, especially whenever there is a disruption or total failure in the IT systems or network infrastructure.

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

Chapter 1

Introduction

Chapter 1

Introduction

1.1 Overview

Mater Dei Hospital (MDH) is a 1,000 bed hospital that provides the public with acute health care services. It complements the services provided by the Gozo General Hospital (GGH), Sir Paul Boffa Hospital (SPBH), Sir Anthony Mamo Oncology Centre (SAMOC), Karin Grech Rehabilitation Hospital and Mount Carmel Hospital (MCH) with the aim of:

- "*providing a patient-centred, quality and timely acute health care service to patients requiring treatment at MDH*" by:
    - providing a service in line with medical advancements;
    - an appropriate complement of qualified, motivated and dedicated professionals;
    - providing a teaching/training programme to all medical, nursing and paramedical staff; and
    - using key clinical performance indicators in line with international standards.
- "*providing health services that support and integrate with the other health-related services through a multi-disciplinary approach*"
    - to sustain a collaborative working model that integrates with all system partners.
- "*maintaining the highest standards of governance ensuring that sustainability and value for money of the operation of the hospital*" through:
    - an appropriate institutional framework;
    - IT systems and management control systems;
    - payroll management;

- procurement management;
- equipment management;
- internal audits; and
- maximising utilisation of resources.

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

1.2 Organisation Structure

The primary aim of MDH is to create a centre of excellence in the provision of effective and efficient, acute patient centred quality care. Furthermore, MDH aims to achieve high levels of patient and staff satisfaction, and enhance research and innovation in a number of specialities. From a clinical perspective, these functions fall under the responsibility of the Clinical Director and are subject to the supervision of the Medical Superintendent of MDH as depicted in the Organisation Chart (Appendix A).

MDH operates an accident and emergency service that handles approximately 300 patients per day, of which approximately one third are admitted as inpatients. Furthermore, it operates between 42 and 45 inpatient wards depending on the influx of patients (temporary wards are created when the number of patients recovered at the hospital exceeds the available bed space) and is equipped with 33 operating theatres to cater for emergency and elective surgery services.

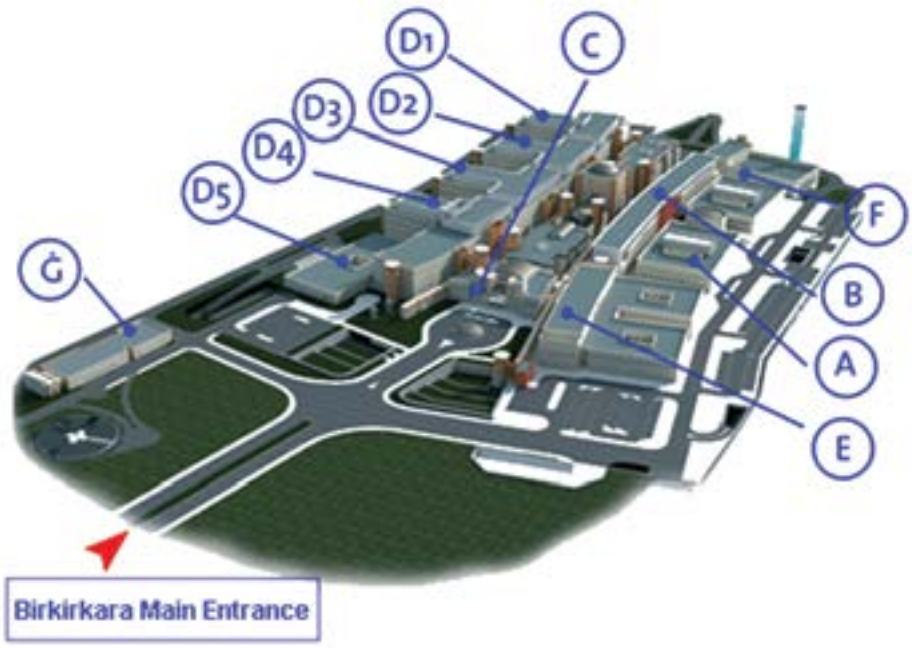


Figure 1 – MDH Layout

As depicted in Figure 1, MDH is divided into a number of blocks, namely:

- Block A – Auditorium, Medical School, Faculty of Health Sciences and MDH Administration, which is occupied by the Office of the Chief Executive Officer (CEO), Advisors and Directors, Nursing Administration, the Procurement, Finance and Payroll departments, and the Human Resources and Administration.

- Block B – Staff Facilities (Changing Rooms and Showers), Laboratories and the Department of Pathology, Renal Unit, and the Rehabilitation services for MDH patients, which include Physiotherapy and Occupational Therapy.

- Block C – Main Entrance, Chapel Auditorium, On-Call Staff Facilities, Offices, Staff Restaurant, Radiology Department, Sterilization Department, Public Facilities such as Customer Care Desk, Kiosks, Public Cafeteria and ATMs.

- Block D – Accident and Emergency Department, Observation Admission Unit, Inpatient Wards, Day Care Unit, Catheterisation Suite and the Hyperbaric Unit. Moreover, Block D is further split into four blocks, whereby each block has been colour coded to facilitate orientation within the Block.

    - Block D1 (Blue) – Ophthalmic Ward, Urology Wards 1 and 2, Sleep Lab, Paediatric Day Care Unit, Neonatal and Paediatric Day Care Unit, Day Care Unit, Day Care Surgery Unit, Surgical Ward 5, Obstetrics Ward 3, Delivery Suites, Disneyland, Wonderland, and the Rainbow Unit.

    - Block D2 (Green) – Surgical Wards 3 and 4, Gynaecology Ward, Delivery Suites, Ear, Nose and Throat (ENT) Ward, Obstetrics Wards 1 and 2, Operating Theatres, Fairyland and the Orthopaedic Ward 3.

    - Block D3 (Yellow) – Plastic Surgery and Burns Unit, Surgical Wards 1 and 2, Orthopaedic Wards 1 and 2, Neuro Surgical Unit, Neuro Medical Unit, Catheterisation Suite and the Medical Ward 6.

    - Block D4 (Brown) – Medical Wards 1 to 5, Medical Admission Unit 4, Cardiac Medical Ward, Cardiac Surgery Ward, Cardiac Intensive Care Unit, Critical Cardiac Care Unit, Intensive Treatment Unit, Medical Investigations and Treatment Unit, Infectious Diseases Unit, and the Psychiatric Unit.

    - Block D5 (Red) – Accident and Emergency Unit, Observation Admission Wards, Hyperbaric Unit and the Medical Admission Unit 1 to 3.

- Block E – Pharmacy, Infection Control Unit, Outpatients and Seminar Rooms.

- Block F – Fire and Security Systems, Generators, and Engineering Systems.

- Block G – Mortuary.

At the time of this IT audit, MDH has a staff compliment of 4,375 personnel, as depicted in Table 1 below, of whom 323 employees work on reduced hours, whilst 17 employees were offered teleworking facilities.

Position	Full Time		Part Time		Contracted		Total
	Males	Females	Males	Females	Males	Females	
Medical	836	1,788	13	57	287	257	3,238
Non-Medical – Administrative	64	125	0	0	3	3	195
Non-Medical – Technical	242	47	0	0	2	0	291
Others	401	249	0	0	0	1	651

Table 1 - Staff Compliment

1.3 Legislation

To carry out its functions, MDH refers mainly but not exclusively to the following legislations:

- Chapter 458 – Medicines Act
- Chapter 464 – Health Care Professions Act
- Chapter 465 – Public Health Act
- Chapter 528 – Health Act

Furthermore, MDH is also regulated by the following legislations:

- Chapter 9 – Criminal Code
- Chapter 12 – Code of Organisation and Civil Procedure
- Chapter 16 – Civil Code
- Chapter 174 – Financial Administration and Audit Act, and Subsidiary Legislation 174.04 – Public Procurement Regulations
- Chapter 440 – Data Protection Act
- Chapter 452 – Employment and Industrial Relations Act
- Chapter 497 – Public Administration Act
- Chapter 527 – Protection of the Whistleblower Act

1.4 ICT within Mater Dei Hospital

Since MDH provides health care in a number of specialities, MDH is increasingly dependent on ICT to carry out its functions and to process, store and maintain considerable amount of data.

In this regard, apart from the Office Automation (OA) software applications, MDH has around 175 IT application systems. However, for the purpose of this IT audit, the NAO has evaluated 14 IT application systems listed below, which are deemed critical across MDH.

- Access Dimensions – is mainly used by the Pharmacy, the Materials, Management and Logistics (MM&L), the Finance department and all the clinics, wards and stock control departments to replace the nominal and purchase ledgers and the old manual accounting system.

- Central Theatre Management System (CTMS) – is used to automate the process by which Consultants manage their patient waiting lists and for management to monitor the progress of the patient's waiting lists.

- Centricity PACS – stores, views, modifies and transfers medical images acquired for clinical investigations. These images are derived from examinations such as PET-CT scans (which combines images from a Positron Emission Tomography (PET) and a Computed Tomography (CT) scans that are performed at the same time using the same machine), Mammography, Magnetic Resonance Imaging (MRI), X-rays etc. These images are sent to PACS from the various modalities and are then stored in a database.

- Centricity RIS – is the backbone software application used by the Medical Imaging Department to address the radiology workflow needs.

- Cardiovascular Information System (CVIS) – has a number of clinical modules that captures data during diagnostic, therapeutic and follow-up examinations, which are then stored in a single relational cardiovascular database.

- CPAS – is the backbone application of all the health systems. It stores patient demographics and episode tracking, inpatient and outpatient appointments, nurses time-off-in-lieu, and various other modules.

- Dakar – provides payroll processing of all MDH employees, which includes the maintenance of MDH's employee details and keeps track of employees' schedules, attendance sheets, the management of leave, time-off-in-lieu, allowances and the actual payroll calculation.

- DCU application – is mainly used by nurses and doctors within the DCU to create, modify or search for a patient appointment or to input patient results for patients who are under medical observation at the DCU.

- Electronic Case Summary (ECS) – is mainly used by doctors to compile inpatient discharge letters electronically.

- iSoft Clinical Manager (iCM) – is a consolidated database of electronic clinical patient information that provides patient demographic data, visit history, order entry, results viewing, patient documentation, etc.

- ID Tag System – is used to issue identification tags for all MDH employees or other third party employees who are giving a service to MDH on a daily basis.

- Laboratory Information System (LIS) – provides the computerisation of several laboratory processes and renders pathology reports electronically available to other hospital systems.

- Online Requisition System (ORS) – is mainly used to create requests and order stock items for the MM&L department, Pharmacy and all the clinics and wards within MDH.

- Online Surgical Register (OSR) – is used by the operating theatre clerks to input all the information that is recorded manually in the operating theatre register.

In addition, the NAO also reviewed the management and maintenance of the MDH's website and Intranet portals, MDH Facebook page, the myHealth website and the ICT infrastructure, which include:

- PCs and laptops – MDH has around 1,700 PCs and 100 laptops installed with Microsoft Windows version 7, 8 or 8.1 operating system.

- Servers and Data Storage Equipment – MDH has a number of physical servers and network attached storage (NAS) devices installed in a dedicated server room that is managed by the IM&T unit.

- Local Area Network (LAN) – MDH is connected to the Malta Government Network (MAGNET) through a fibre-optic connection.

- Wi-Fi network – MDH has a third party Wi-Fi connection that is managed by the IM&T unit and is only accessible by the CEO and the Directors within the Administration Block. Having said that, MDH has a few other third party Wi-Fi connections installed in different areas within MDH, which and are managed by the respective third party suppliers.

- Electronic mail (e-mail) system – MDH utilises the Government's e-mail system.

- OA software applications – All the Microsoft software licences are acquired through the MITA under the Government Enterprise Agreement and the respective licences are managed by the Information Management Unit (IMU) within MEH.

1.5 Audit Scope and Objective

The scope of this IT audit was to analyse the IT and Information Systems used within MDH, to determine whether MDH has the necessary controls to maintain data integrity, safeguard assets, allow organisational goals to be achieved effectively and to ensure the efficient use of the Government IT related resources. The audit report identified any potential risks and made the necessary recommendation to mitigate those risks. However, given that the scope of this audit was to carry out an IT audit, the review of the selected software applications should not be considered as a detailed Information Systems audits. Such audits would normally be carried out as a standalone review for a particular system.

The IT audit was divided into three different stages:

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

- The NAO then went through MDH's overall strategic direction, objectives, internal structures, functions and processes to gain a comprehensive understanding of MDH and its environment. This included in-depth interviews with key officials and stakeholders, as well as observations, reviews of user manuals and other documents requested in the pre-audit questionnaire.

- The third stage examined how the IT applications are being used to achieve their objectives. In this regard, the IT audit went through the processes and procedures related to every software application and reviewed whether these software applications were properly maintained. Furthermore, the IT audit looked into the physical and logical access controls, adherence to policies, standards and procedures, network infrastructure, security controls and for any Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) that exist.

Therefore, the objectives of this report were to:

- document all the information collected during the various interviews held with a number of key stakeholders and officials;

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

- determine whether MDH's IT systems selected for the purpose of this IT audit operate effectively, efficiently and economically;

- list all the findings and identify any potential risks; and

- list all the recommendations to mitigate those risks.

1.6 Audit Methodology

To achieve the above objectives, a pre-audit questionnaire was sent to MDH and a number of interviews were held with key officials at MDH and the Ministry's IMU (Health) between Q2 – Q3 2015. In addition, drafting of the report was carried out between Q4 2015 and Q1 2016.

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

1.7 Structure of the Report

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

- Chapter 2 covers the IT governance and the management of the IM&T unit by evaluating the manner in which ICT resources are managed.

- Chapter 3 reviews a number of software applications that were sampled for the purpose of this IT audit.

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

- Chapter 5 analyses whether MDH is managing and controlling its IT operations in the most effective way. Furthermore, it addresses MDH's level of confidence with any BCP or DRP in the event of a service disruption.

- Chapter 6 lists all the management comments submitted by MDH.

1.8 Acknowledgement

The NAO would like to express its appreciation to the MDH's CEO and all the staff within MDH, in particular the Director Health Informatics, all the key officials within the IM&T unit, and the Directors and key officials within the respective units, who were involved in this audit. Furthermore, the NAO would also like to thank the Chief Information Officer (CIO) and key officials within the Ministry's IMU (Health), for their time and assistance.

Chapter 2

IT Management

Chapter 2

IT Management

2.1 Information Management and Technology Unit

The Information Management and Technology (IM&T) unit is headed by the Director Health Informatics, who was appointed to this post on the 15th of September 2014, and reports directly to the Director General Health Care Services and MDH's CEO. The aim of this unit is to:

- provide first-line IT support on a number of hardware devices and software applications that are not supported by any service contract;
- process new requests for hardware installations;
- carry out system analysis;
- maintain a number of key systems and applications;
- advice business users on any ICT requirements;
- adhere to the Data Protection rules;
- collect and provide data as required;
- serve as the custodian of Medical Records;
- keep an updated hardware inventory of all the ICT assets within MDH;
- liaise with the Ministry's IMU (Health) and MITA on any IT projects.

The NAO observed that there is a very good level of communication between the Director Health Informatics and key officials within this unit, whereby meetings are held every month to discuss any issues or to provide useful information of any forthcoming changes/enhancements that are to be

implemented on MDH's ICT infrastructure. The same level of communication exists between the IM&T unit and the Ministry's IMU (Health), MITA and third party suppliers.

At the time of this IT audit, the IM&T unit is made up of 72 officials, and is divided into a number of units, as depicted in Appendix B.

2.1.1 CPAS Team

The CPAS team consists of one clerk carrying out the duties of a System administrator assisted by two other clerks. The role of the CPAS team is:

- to offer first-line technical support to all the end users at MDH and other entities within the MEH who have been granted access to the CPAS application;
- the overall administration of the system, which includes, the management of user accounts and user roles, the management of the outpatient booking system etc.;
- to carry out system testing whenever a new functionality has been added to the CPAS application;
- to liaise with the CPAS database administrator and the CPAS software developer when applicable; and
- to offer user training when required or to schedule refresher courses from time-to-time.

The CPAS team also offers a Helpdesk functionality within MDH, whereby the end users can phone directly whenever assistance is required. However, the NAO was informed that the end users are instructed to phone MITA's Service Call Centre whenever a problem crops up on CPAS, since calls are not being recorded whenever an end user has a problem and requires assistance. Thus, whenever an end user phones MITA's Service Call Centre, an incident request is raised in MITA's Call Logging system and is then escalated to the CPAS team. In turn, the CPAS team have access to MITA's Call Logging system and would then service the request accordingly. In this regard, the NAO is of the opinion that unless the calls are logged through the proper channels, the CPAS team cannot substantiate the level of support being provided and quantify exactly the number of incident requests that were serviced periodically.

2.1.2 Data Management Unit

The Data Management Unit (DMU) consists of the Manager Clinical Coding and Data Quality and three members of staff. The role of the DMU is to process clinical data for clinical research, epidemiology, health resource allocation and public education.

Thus, for the data to be recognised both locally and internationally, it is clinically coded using international classifications. Clinical coding is the translation of medical terminology, as written by the clinician, to describe a patient's complaint, problem, diagnosis, treatment or reason for seeking

medical attention into a coded format. The latter can be easily tabulated, aggregated and sorted for statistical analysis in an efficient and meaningful manner and consequently be compared with other data locally and internationally.

The DMU ensures accuracy and consistency of information produced during the clinical coding process and that the data is entered in a timely manner. The NAO observed that the DMU deals mainly with four types of hospital data:

1. **Hospital Activity Analysis (HAA)** – this was established in 1992 with the aim of collecting and collating data regarding hospital activity. The HAA system originated in every ward whereby staff were requested to fill in an HAA form for every inpatient or day case on discharge from hospital. These manual forms were then forwarded to the DMU, to be checked with the former CPAS application for demographic details, clinically coded and entered in the HAA database, before they are validated.

   With the introduction of the ECS, in January 2009, this contributed to an improvement in the accuracy, completeness and timeliness of inpatient activity data, direct clinical coding of patient diagnosis on the system and reduced the need of filing and archiving space and the use of paper.

   In June 2010, a new HAA form was created by the DMU to be filled in for cases for which no ECS was previously issued. This is filled in for those patients who are admitted to Cath Lab, Obstetric Wards, Paediatric Day Care Unit and Rainbow Ward, where patients attend on a frequent daily basis for treatment purposes.

   In September 2010, the DMU started registering deceased patients, inputting the data directly from copies of death certificates onto the HAA database. Previously, no HAA form was filled in for most cases by the respective wards, with an adverse effect on hospital statistics.

   The HAAs are clinically coded by the DMU using the International Classification of Diseases and Related Health Problems (ICD-10), which is a classification of causes of morbidity and mortality issued by the World Health Organisation (WHO).

   At the time of the IT audit, the DMU processed around 6,500 HAAs monthly. The manual HAAs and those issued from the ECS, are clinically coded and validated for use by the Clinical Performance Unit within MDH, in the production of its monthly and annual reports.

2. **Surgical Procedures** – all the data retrieved from the surgical operations register is clinically coded by the DMU using the International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM) and categorised according to the British United Provident Association (BUPA) '*Classification of Surgical Procedures*' into Complex Major, Major +, Major, Intermediate or Minor Category. These are then validated by the DMU for use by the Clinical Performance Unit for the production of their monthly and annual reports.

   In this regard, the NAO was informed that every month, the DMU processes around 4,700 surgical procedures that are performed at MDH. Furthermore, the DMU records the '*Cancellations of*

Surgical Procedures' at MDH, which amount to approximately 120 a month. These cancellations are categorised according to the BUPA Classification of Surgical Procedures and the Reason for Cancellation.

3. **CTMS** – In April 2015, the DMU triggered the process of clinically coding all the surgical procedures for all specialities that were inputted in the CTMS according to ICD-9-CM. This amounted to approximately 19,000 cases dating back to 2002. This list increases by approximately 3,500 cases per month.

4. **CPAS** – the DMU assists the CPAS Team in updating the CPAS application with any missing or incorrect patients' demographic details. Between January and February 2015, around 15,240 date-of-births were checked and some were modified, whilst in March 2015, 3,419 deaths were verified and registered as deceased on the CPAS application.

Taking into consideration the amount of data that is handled and processed manually every month, the NAO commends the dedication shown by the DMU to ensure accuracy and consistency of data, which is essential for management, as it forms the basis for the reports prepared and issued by the Clinical Performance Unit and other departments within MDH.

2.1.3 ICT Application Support

During the course of the IT audit, a number of interviews were held with seven officials, each having the role of an ICT Application officer, ICT Engineer, Hospital IT System administrator or ICT Manager within the IM&T unit. Their function within the IM&T unit is critical in nature, since they are responsible for the overall management of a number of software applications in use within MDH, including Access Dimensions, CTMS, ECS, iCM, ORS, OSR, PACS, and RIS amongst others and are also involved in:

- carrying out system analysis;
- performing software compatibility testing and configuration;
- the development of ad-hoc reports;
- the development of in-house software applications;
- providing user training;
- offering first-line of support to the end users;
- liaising with MITA or third party suppliers when applicable; and
- attending to Senior Management meetings when required.

The NAO observed that most of the above functions are not carried out as a team but taken care of by individuals according to their area of responsibility. Whilst the NAO commends every individual for

the level of professionalism and dedication in their work, during the course of the IT audit, the NAO was informed that some of these officials were even assigned the duties of the IM&T Networks team. This task was entrusted to some of these officials because both officials within the Networks team had resigned. In this regard, the NAO recommends that apart from the fact that sufficient human resources should be engaged to fill-in the posts vacated within the Networks team, the above functions and the overall management of any software applications should not be dependent on one individual. Thus, taking into consideration the criticality of the functions of the IM&T unit, MDH should also ensure that sufficient level of human resources are allocated to this unit.

2.1.4 IT Services Support

The IT Services Support team consists of a senior clerk and two clerks who are responsible to raise an electronic Request for Service Form (eRFS) with MITA for the creation, modification or deletion of a Domain user account and to grant or remove access to a particular folder stored on the MDH network on behalf of the end user. The IT Services Support team also acts as a liaison between MITA and the Ministry's IMU (Health) on behalf of the end users, and is responsible for managing the end users' service contracts.

Whenever new users are to be employed within MDH, the IT Services Support Team will raise an eRFS with MITA for the creation of a Domain account, so that the end user can log on to the network and access the Government's e-mail and Internet services. Through the eRFS, the IT Services Support Team informs MITA whether the user needs to be granted access to a particular folder stored on the MDH network and whether the end user requires access to any of MDH's critical systems such as CPAS and iCM. The NAO observed that the IT Services Support Team keeps track of all the eRFSs with all the requests being recorded in a database. The end users are then informed by e-mail or phone, once a Domain user account is created or access to a specific folder has been granted, and whether the end user is required to attend to training on the use of MDH's critical systems.

During the course of the IT audit, the NAO observed that in Q1 2015, MDH started a process to verify whether there are any inactive user accounts, which need to be deleted. In this regard, MITA has drawn up a report of all the active and non-active Domain user accounts and forwarded it to MDH to take the necessary actions. The IT Services Support Team goes through the list of inactive Domain accounts listed in this report and for each user verifies whether he/she is still listed in the MDH payroll through the Dakar application. There may be instances whereby:

- a user account is inactive but the end user might still be on MDH payroll (ex. parental or long vacation leave);
- a user account which is rarely used but needs to be kept active (ex. visiting Consultants);
- a user account is active but the end user cannot be found under the MDH payroll (ex. subcontractors who are giving a service to MDH).

In such instances, the IT Services Support team carry out various checks with different stakeholders to ensure whether an active or inactive Domain user account needs to be retained before raising an eRFS with MITA for the deletion of the respective user account. Whilst the NAO commends this initiative in the management of user Domain accounts, the NAO recommends that this should be done as part of an on-going process and not a one-off exercise. Furthermore, once it has been established that a Domain user account is no longer in use and needs to be deleted, the same procedure should be applied on all the software applications in use within MDH to ensure that the user account is deleted by the respective System administrator.

2.1.5 IT Technical Support

The IT Technical Support team is headed by a senior systems administrator who is assisted by two acting senior technical officers and three self-employed technical officers. The aim of the IT Technical Support team is to provide second-line technical support to all the end users within MDH and SAMOC and is mainly involved in:

- the relocation of offices;
- configuration, testing and the setting up of new hardware and software applications;
- servicing and repairs of IT equipment which are not under any maintenance contract;
- the replacement and disposal of any hardware equipment;
- assisting in the patching of network points and connecting IT-related equipment to the Government network;
- ensuring that the hardware inventory is continuously updated;
- constant liaising with the Ministry's IMU (Health) to ensure that all the hardware covered by the Government maintenance contract is updated in the centralised Asset Management System (AMS) owned by MITA; and
- providing technical assistance in compiling hardware specifications prior to an Invitation to Tender (ITT) or involved in the adjudication stage of IT-related equipment.

The IT Technical Support team also has a sub-contractor whose main responsibility is to provide first line technical support on any hardware/software related issues encountered on any of the PCs or laptops installed at MDH, which are covered by a Government maintenance contract. In this regard, the end user would raise an incident request with MITA's Service Call Centre, who in turn would then escalate the incident request to the MDH's sub-contractor. The NAO observed that on average around 20-30 incident requests are raised by the end users on a daily basis and the sub-contractor is on-call in the event that an urgent request is raised after office hours.

2.1.6 IT Trainers

The IT Training section consists of an ICT Support Officer carrying out the duties of an IT Trainer and a senior clerk who is responsible for the scheduling of training and the management of the training room whenever the training facilities are required.
The NAO observed that the IT Training section offers training on some of the major software applications in use within MEH, namely ECS, iCM, PACS and ePortfolio. The latter was designed as a learning tool for foundation doctors to be able to plan and manage their Foundation Programme.

Training is tailored specifically to meet hospital staff requirements and is delivered either one-to-one or in groups. One-to-one training that is delivered on site both if, the individual works in a particular ward at MDH and even if the individual works outside MDH, such as in Health Centres, GGH or MCH. One-to-one training is also delivered in the IT training room, although the latter is normally used to deliver training in groups. In this regard, the IT training room is equipped with five PCs and two laptops and has a seating capacity of 15 individuals. However, if hands-on-training is required, only eight individuals are accepted.

Unfortunately, due to the lack of resources, the IT Training section normally schedules at least one or two lectures a day during office hours. In this regard, the NAO recommends that training should not be dependent on one IT Trainer and ideally, other resources are recruited to be able to provide continuous support on the software applications and assist the end users through the initial stages of using the software application.

During the course of the IT audit, the NAO observed that the ICT Support Officer took the initiative to create user manuals and pamphlets for the end users attending to training and which can also be downloaded from the IT Trainers portal. Through this portal, the end user can also download downtime forms. Thus, in the event of a system downtime the end users must follow the system downtime procedures, whereby all the transactions must be recorded in the respective form, to facilitate data entry when the system is back to normal. The IT Trainers portal was designed and is being maintained by the ICT Support Officer. Whilst commending this initiative and taking into consideration the lack of resources, the NAO recommends that, the IT Training section should consider offering e-Learning or m-Learning facilities to the end users according to their job function within MDH or other sites within MEH through the IT Trainers portal.

2.1.7 Medical Illustrations Unit

The Medical Illustrations unit was set-up in 2008 and is headed by a Clinical photographer and a clerk. The primary function of this unit is to take clinical photos and videos of patients to help with their diagnosis and treatment. In this regard, the Medical Illustrations unit follows strict consent policies and thus, the procedures of taking photos or videos of the patients and their subsequent use are explained in detail to the patients. Depending on the level of consent given by the patient, the images can also be used for educational purposes, especially in case of rare diseases, and also published in reputable medical journals. In this regard, the NAO recommends that the patient's consent should always be given in writing by the patient him/herself or a member of their family and should not be accepted verbally.

The unit is also equipped with video conferencing facilities, which are used for teaching purposes as well as for telemedicine purposes. Since the Unit has links with foreign universities and foreign hospitals, health care professionals or students can attend webinars within MDH by means of fixed or portable webcams, thus eliminating days lost due to travelling and related expenses. Other facilities include the capability of transmitting live surgery from the operating theatres to the Medical Illustrations unit's videoconferencing rooms. Surgeons can explain what is happening and even take questions from students or other professionals during a particular intervention. The video conferencing facilities, are also used by local medical consultants to collaborate with other foreign consultants to discuss particular patients. The foreign consultants are able to view the patient as well as the electronic clinical findings in real time whilst being able to speak to both the patient and his/her local consultant, thus reducing the need to bring specialists to Malta or fly patients to hospitals abroad.

Apart from photographic and videographic equipment, the Medical Illustrations unit is also responsible for the graphic design of patient leaflets, booklets and educational large format posters. These are printed in-house using high volume digital colour printers and wide format printers, for a quick turnaround.

2.1.8 Medical Records Department

The Medical Records department is the custodian of medical records, which is made up of documents related to the patient's clinical history. These include doctors' notes, nursing reports, blood investigations and medical reports including any imaging investigations like ultrasound and X-rays. All these are collected in one medical file bearing the patient's ID card number, name, surname, and the name of the hospital or clinic, where the treatment was received.

At the time of the IT audit, the Medical Records department was made up of 44 personnel, most of them working on different rosters. The Medical Records department consists of two main libraries, and apart from being the custodian of medical records, has a number of functions within MDH, which include:

- the registration of newborns and foreigners admitted for the first time at MDH;
- the creation of a new physical file for newborns or any patient admitted for the first time at MDH, including any foreigners;
- the updating of records to merge or change the hospital number;
- the recording of all patient file loans and returns from and to the Medical Records department, in the CPAS application;
- the repairing of patient's files due to wear and tear on frequent use, including the opening of new patient file volumes where necessary;
- the preparation of patient's files for MDH Wards/Units, Health Centres, SAMOC, SPBH, GGH, Karin Grech Rehabilitation Hospital, St. Vincent de Paule Residence (SVPR), and audits.

- the preparation of patient's files two weeks in advance prior to an individual's outpatient appointment at MDH;

- the archiving of patient's files, which are either marked inactive from the CPAS application or patients' files of deceased persons. The latter patient's files are retained for a period of 10 years at the Medical Records department's archive;

- the filing of X-ray image reports of patients, which are normally generated by other Health entities who do not make use of the Medical Imaging applications;

- the filing of investigations; and

- the issuing of various statistical reports from time-to-time.

Apart from MDH patients' files, the Medical Records department also retains (and retrieves) physical files of patients admitted at SAMOC, at the Orthopaedic Clinics across the Health Centres, at the Cardiovascular Clinic in Ħas-Serħ, as well as X-Ray films taken at Health Centres since 2010. However, the NAO was informed that the volume of X-Ray films taken at Health Centres is diminishing, since Health Centres are in the process of switching to an online-digitised application. As depicted in Figure 2 below, the Medical Records department has 196,377 active patients' files, whilst the Medical Records archive has 157,680 inactive patients' files, 52,759 X-Ray films and 50,022 files pertaining to deceased patients.

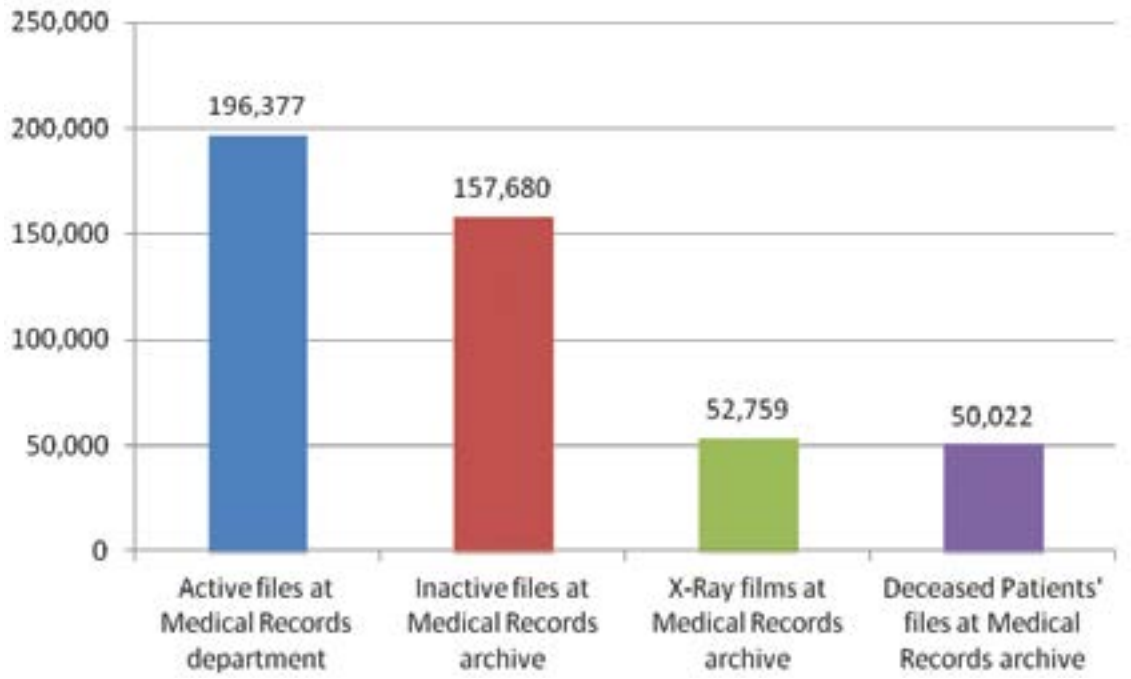


Figure 2 – Number of files at Medical Records

During the course of the IT audit, the NAO observed that all these patients' files are stacked (and filed) according to the patient's ID card number in a number of shelving systems, which are almost packed to their full capacity. As a result, the Medical Records department is running out of space and will soon be finding it difficult to stack more patients' files. In this regard, the NAO was informed that the Medical Records department, together with the Director Health Informatics and the MEH are looking for options to provide a simpler way of storing patients' health information. In view of this, discussions are underway on the possibility of implementing a digitised system, whereby patient's health information is scanned and saved electronically.

File movements	Totals	Average per month
Files on loan	564,951	47,079
Files returned	503,199	41,933
X-Ray films	11,269	939
Files repaired/Volumes created	356	30
New files created	10,466	872
Filing of investigations	27,258	2,272

Table 2 - File Movements - 2014

In the meantime, the NAO observed that the Medical Records department generates a number of reports on a regular basis. As part of the audit process, the NAO was provided with a statistical report on the file movements for 2014. As depicted in Table 2 above, in 2014, the Medical Records department issued 564,951 patient files on loan to various wards and outpatient clinics within MDH, other hospitals (ex. GGH, SPBH) and Health Centres, with an average of 47,079 patient files a month. Similarly, the total number of patient files, which were returned from loan, amounted to 503,199 with an average of 41,933 patient files a month. Taking into consideration the laborious work in handling all these patient files and the recording of these files manually in CPAS, the NAO recommends that MDH evaluates the options either of implementing the concept of RFID (Radio Frequency Identification) tagging of patient files or implementing a document management system, whereby patient's health information may be scanned and saved electronically, thus reducing the volume of the physical files and the related storage space required.

2.1.9 Networks Team

The Networks Team was made up of an ICT Support Officer and a sub-contractor taking the role of a Junior System administrator. The Networks Team played an important role within the IM&T unit and was responsible for a number of functions, which include:

- acting as a liaison between MDH and MITA on any issues related to the network infrastructure;
- acting as a liaison between MDH and local third party suppliers on any issues related to the hardware equipment installed at the MDH server room;
- being involved in the planning of the migration of a number of IT applications systems, installed on MDH servers, on to MITA's SHE;

- carrying out risk assessments and the drafting of a number of Standard Operating Procedures (SOPs);

- liaising with the Engineering Department on any issues related to the air-conditioning and fire suppression systems installed at the MDH server room. The Networks Team also liaises with the Engineering Department whenever there is an unexpected or scheduled power cut, to ensure that the Generators kick-in and the IT equipment installed at the MDH server room is unaffected by the scheduled/unexpected power cut;

- managing a number of virtual environments hosted on servers at the MDH server room;

- managing user accounts and granting user privileges to folders accessible on the MDH network infrastructure;

- monitoring and upkeeping of the MDH server room; and

- scheduling and monitoring of the daily/weekly/monthly backups.

During the course of the IT audit, both the ICT Support Officer and the Junior System administrator resigned from MDH. In this regard, the Director Health Informatics had to find a remedial solution and appointed a number of ICT Application officers within the IM&T unit to assist with the daily operations of the above functions.

2.2 Information Management Unit

The primary role of the Ministry's Information Management Unit (IMU) (Health) is to ensure the alignment of IT with the Ministry's business priorities and to provide support and advice to the Permanent Secretary on all ICT matters. The functions of the IMU include:

- the preparation of strategic and operational ICT plans for the Ministry in line with the National ICT Strategy;

- providing support and advice to the Permanent Secretary on ICT matters;

- providing technical advice about the procurement and/or leasing of ICT-related equipment;

- co-ordinating the upgrading, development and implementation of new Information Systems;

- the preparation of the ICT budget and the optimisation of ICT resources; and

- the involvement in applying Government-wide policies, standards and protocols, which are aimed at ensuring that IT systems are mutually compatible.

The Ministry's IMU (Health) is managed by a CIO, who was appointed to this post in 2013. The NAO was informed that in 2012, the IMU had a staff compliment of 22 officials, however, at the time of the IT audit, only 12 officials were still working at the IMU. The main responsibilities of this unit include:

- providing strategic assistance to the CIO;
- acting as the IMU liaison for European Union (EU) related matters and projects, and for the Electronic Exchange of Social Security Information (EESSI);
- liaising with the IM&T unit, MITA and local third party suppliers on any ICT related issues or forthcoming projects at MDH;
- liaising with various stakeholders on ICT matters related to the Department for Health Regulation and Directorates, St. Luke's Rehabilitation services, GGH's Campus network, Dar Kenn għal Saħħtek, FMS and other Health Entities;
- defining specification requirements for IT related equipment and participate in adjudication boards for the evaluation of bids;
- managing the procurement of workstations and licences through the Government Centralised Procurement framework;
- the upgrading of workstation operating systems, e-mail client and line of business software when applicable;
- the installation of non-standard software through the Software Installation and Request Assessment;
- the auditing of workstations installed within the Health portfolio and re-deploy workstations accordingly;
- maintaining the Ministry's AMS for the upkeep of workstations inventory throughout the Health portfolio;
- the overall management and upgrading of websites and online facilities (when applicable), such as the Health website (**http://www.health.gov.mt**), the myHealth website (**http://www.myhealth.gov.mt**), eForms and KURA;
- providing first-line support to doctors and patients on the myHealth website, through the myHealth generic mailbox or phone, and to offer first-line response and investigation of incidents related to myHealth website; and
- providing the necessary support for the continued operation of core health systems to ensure that systems software and hardware have appropriate maintenance and support services contracts.

During the course of the IT audit, the NAO observed that the Ministry's IMU (Health) maintains a very good working relationship and a high level of communication with the IM&T unit on any ICT related matters within MDH.

2.3 IT Strategy

An IT strategy is an integral part of the overall organisational strategy. It is typically a long-term action plan that guides organisations on how technology can help them achieve their goals, boost their competitiveness and increase their chances of success through technological innovation, cost savings and process automation.

The IT strategy should consider all facets of technology management, including cost control, skills, hardware, software, risk management and other areas of IT, as well as how investments in these capabilities support the overall business strategy. An effective IT strategy should allow IT to be flexible enough to adapt to changing business priorities, available skills and budgets, new technologies and evolving user and customer needs.

As a result, defining an effective IT strategy can be complex. However, if it is well planned, any organisation can notice a great deal of technology-driven changes. Once an IT strategy is defined, it should be revisited often to ensure that the organisation has made the right technology investments and that these investments align with the business strategy.

During the course of the IT audit, the NAO was informed that the IM&T unit had drafted an IT strategy for MDH, in line with the Ministry's IT strategy. At the time of the IT audit, this IT strategy still needed to be finalised and approved by the Ministry. In this regards, the NAO recommends that the IT strategy is given its due importance, and is finalised and approved by the Ministry as soon as possible.

2.4 ICT Budget

The ICT Budget is assigned through the Ministry's IMU (Health) following a number of discussions between the Director Health Informatics and other key stakeholders within MDH. The ICT Budget is formalised after taking into consideration MDH requirements in terms of any IT-related projects that need to be implemented within MDH. These IT-related projects may require ICT support or investment in the current IT systems, which may need to be replaced or upgraded, the procurement of new ICT peripherals, office communications and other ICT equipment or the investment and implementation of a new software application system within MDH.

2.5 Product Lifecycle Management

The product lifecycle management is a systematic approach to managing the series of changes a product goes through, from its design and development to its disposal. In this regard, the NAO reviewed the process involved in the procurement, maintenance and disposal of ICT hardware equipment and the planning, development, acquisition, testing, implementation and maintenance of software applications within MDH.

2.5.1 Hardware Lifecycle

The hardware lifecycle is a holistic approach to managing the total useful life of IT hardware components from the procurement stage to the disposal of asset.

2.5.1.1 Procurement

The NAO was informed that once the specification requirements for IT related equipment are defined, the IM&T unit co-ordinates and procures the relative IT equipment through the Central Procurement and Supplies Unit (CPSU). However, whenever new PCs or laptops are required, the IM&T unit will liaise with the Ministry's IMU (Health), who will then manage and procure the PCs and laptops, and their respective software licences, through MDH funds via an established contract with MITA.

In this scenario, MITA issue a quotation to the Ministry's IMU (Health), who in turn issue a Local Purchase Order (LPO) and send it to the former. Upon receipt of the LPO, MITA then place the order on behalf of MDH with the respective supplier. The latter then deliver the PCs or laptops at MDH within the established Service Level Agreement (SLA). The IT Technical Support team acknowledge the delivery and commissioning of the PCs and laptops by signing the delivery note, which is sent by the supplier via e-mail to MITA's Procurement Section. Following this, MITA update the Procurement records with the hardware details accordingly and issue an invoice to MDH to effect payment.

2.5.1.2 Maintenance

As highlighted earlier in the report, the IT Technical Support team offers first-line and second-line technical support, which includes the servicing and repairs of hardware, including PCs and laptops procured through the Government centralised procurement framework and any other IT-related equipment, such as stand-alone printers, scanners, PCs etc., which are not covered by any maintenance contract.

The NAO was informed that in the event of a hardware or software malfunction related to the above IT-related equipment, all MDH users are requested to phone MITA's Service Call Centre. If the problem cannot be resolved over the phone, the service request is escalated to the IT Technical Support team. The sub-contractor, within the IT Technical Support team, provides first-line technical support on any hardware or software related issues encountered on any of the PCs or laptops installed at MDH, which are covered by a Government maintenance contract. If following the hardware repair, the PC or laptop requires software re-imaging, this is carried out as part of the hardware repair process.

In the meantime, all the other IT-related equipment, which does not form part of the Government maintenance contract, is serviced and repaired by the IT Technical Support Team. However, if the hardware is still under warranty, the IT Technical Support team will liaise with the respective third party local supplier, to call on-site at MDH and accompany them, whenever servicing or repairs are required. On the other hand, if the hardware is not covered by any warranty or SLA and the service request is escalated to a local third party supplier for repairs or servicing, the IT Technical Support team requests that a quotation is sent to MDH before the item is repaired. Upon approval, the IT Technical Support

team liaises with the Finance department within MDH to issue an LPO for the servicing or repairs of the respective hardware.

The NAO was informed that all the requests for the servicing or repairs of any IT-related equipment are recorded in MITA's Call Logging system and are accompanied by a job sheet and/or invoice whenever a part or consumable is replaced. The NAO observed that the IT Technical Support team keeps a record of all parts or consumables, which were replaced from stock, in an internal database.

2.5.1.3 Disposal

During the course of the IT audit, the NAO reviewed the procedure adopted by the IT Technical Support team for the disposal of IT equipment that is either obsolete or beyond economical repair. The NAO was informed that all the IT equipment, that was certified by the Waste Management Board within MDH, as obsolete or beyond economical repair, is stored in a specific room and disposed of accordingly.

The NAO noted that the IT Technical Support team keeps a record of all the hardware equipment that will be disposed of and formats the hard disk whenever a faulty or obsolete PC or laptop is to be disposed of. However, the NAO observed that the IT Technical Support team does not securely wipe hard disks whenever a PC or laptop is transferred to a different user or disposed of.

In this regard, the NAO recommends that the IT Technical Support team adopts the Government of Malta Information and Communication Technology (GMICT) Desktop Services Procedure (GMICT R 0084:2009)[3] in terms of PCs or laptop disposal and data wiping, and ensures that data on equipment being disposed of could not be retrieved by any third party.

2.5.2 Software Lifecycle

A software lifecycle is essentially a series of steps or phases that provide a model for the development and lifecycle management of an application or piece of software, from an initial feasibility study through maintenance of the completed application. These steps or phases can be characterised and divided up in different ways, as per below:

- **Project planning, feasibility study** – establishes a high-level view of the intended project and determines its goals;

- **System analysis, requirements definition** – refines project goals into designed functions and operation of the intended application, and analyses end user information needs;

- **Systems design** – describes the desired features and operations in detail, including screen layouts, business rules, process diagrams, pseudocode and other documentation;

[3] https://www.mita.gov.mt/MediaCenter/PDFs/1_GMICT_R_0084_Desktop_Services.pdf

- **Implementation or coding** – on receiving the system design documents, the work is divided in modules or units and the actual coding begins;

- **Integration and testing** – brings all the pieces together into an adequate testing environment, then checks for errors, bugs and interoperability;

- **Acceptance, installation, deployment** – this is the final stage of the initial development, where the software is implemented and starts being used;

- **Maintenance** – this is what happens throughout the rest of the software's lifetime, in terms of changes, corrections, additions, upgrades or migration to a different computing platform.

During the course of the IT audit, the NAO reviewed how MDH manages internal software development projects in terms of planning, development, testing, implementation and maintenance. The NAO also reviewed the process how off-the-shelf applications or software applications, which have been outsourced to a third party supplier, are procured.

The NAO was informed that whenever a software application is developed internally, MDH adheres to most of the phases in the software lifecycle highlighted above. In this regard, the NAO was provided with design documents, such as the '*ECS Design document version 2.2*', which included amongst others the business processes, systems analysis and requirements definitions, data flow diagrams, coding designs, the technology and third party components used etc., accompanied by separate user manuals for each software application selected for the purpose of this IT audit. These user manuals are often handed-in to the end users when on-the-job training is provided, and are updated sporadically.

In the meantime, the NAO observed that MDH issues an ITT whenever an off-the-shelf software application needs to be procured or for the development of a new software application by a third party software company. In this regard, MDH liaises with the Ministry's IMU (Health) and MITA to assist when necessary in the requirements gathering phase and the drafting of the tender document. The NAO observed that the awarded third party supplier and MDH adhere to the software lifecycle processes highlighted above and follow the change management procedures whenever any changes or enhancements are required on the live environment.

Whilst the NAO commends MDH on the availability of user manuals and a number of standard operating procedures, MDH must ensure that these documents are always kept updated especially whenever new enhancements are added to the system. Furthermore, the NAO recommends that MDH should keep logs of all the software enhancements carried out in-house, off-the-shelf or third party software applications and logs of any system bugs reported and their respective software fixes.

2.6 IT Asset Management

An IT asset management is a set of business practices for optimising and supporting strategic decision-making within the IT environment whilst also increasing the organisation's understanding of the IT business value. An IT asset management is thus an important part of any organisation's strategy. It usually involves in gathering a detailed inventory of all the hardware equipment and software applications installed in an organisation and then using that information to make informed decisions about IT-related purchases and redistribution. As a result, having a good IT inventory management will help organisations manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases, and thus promoting the harvesting of existing resources.

During the course of the IT audit, the NAO observed that different units within the IM&T unit maintain separate IT inventories according to their area of responsibility. The IT Technical Support team, for instance, maintains two different IT inventories. All the PCs and laptops that fall under MITA's service contract are maintained in the Ministry's AMS. In the event that a new PC or laptop is installed or an existing PC or laptop is no longer in use and has been given to a different user within MDH, the IT Technical Support team will inform the Ministry's IMU (Health) by e-mail to update the Ministry's AMS accordingly. On the other hand, any other equipment, which is not covered by MITA's service contract, such as tablets, scanners, printers etc, is maintained in a separate inventory sheet. The NAO observed that the IT Technical Support team also maintains a separate inventory of a number of stock items that are used for the replacement or repairs of PC/laptop hardware components.

As depicted in Figure 3, at the time of the IT audit, the IT Technical Support team was responsible for around 1,700 PCs and TFT monitors, 100 laptops, 28 tablets, 50 scanners, 800 stand-alone printers, 74 multi-function printers, 30 projectors, 50 TVs, two webcams, 100 medical modalities, three touch screens and four video-conferencing system.

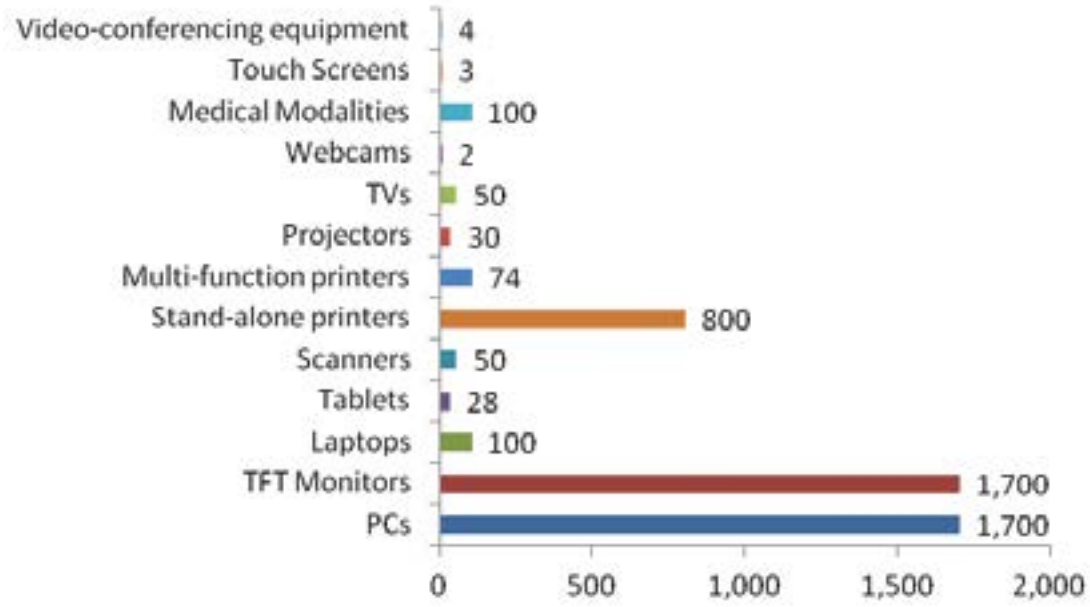


Figure 3 - Hardware Inventory

With regards to the software inventory, the NAO was informed that the IM&T unit, through the Ministry's IMU (Health), procures all Microsoft Windows operating systems and Microsoft Office licenses through MITA, whilst the software licence agreement is renewed annually with MITA.

2.7 Third Party Suppliers

MITA, being the IT Agency for the Government of Malta was entrusted by MDH with the provision of fibre-optic network connectivity to the MAGNET, and provides 24x7 monitoring to this connection, in terms of the core Wide Area Network (WAN) equipment and core access switches. Moreover, MITA also provides MDH with a number of services including:

- the provision of e-mail and Internet browsing and filtering services;
- hosting of Server services and any Guest Virtualised Machines in a segregated environment within MITA Data Centre facilities;
- standard Desktop Security Configuration services, such as Anti-virus, patch management and spam filtering of e-mails via black lists and tagging;
- the provision of Workstation Support services on hardware and software applications;
- the provision of LAN support;
- access to MITA's Service Call Centre for the reporting and resolution of incidents related to the services highlighted above;
- the provision of application support on critical applications in use within MDH, namely iCM, LIS, PACS and RIS; and
- assisting MDH on any IT-related projects.

During the course of the IT audit, the NAO observed that MDH has various other services and maintenance contracts with third party suppliers. Whilst most of the service maintenance contracts that the NAO requested were provided by MDH, the NAO was not provided with a copy of the CPAS service maintenance contract or any related correspondence regarding database support and software development, even though the NAO was informed that both service maintenance contracts were finalised during the course of the IT audit. However, the NAO was informed that the CPAS recurrent yearly costs amounted to approximately €250,000, which cover software licences, development, report generation, and maintenance and support.

Furthermore, the NAO was informed that two software applications, which were selected for the purpose of the IT audit, namely Access Dimensions and the ORS, were not covered by any service maintenance contract.

On the other hand, with regard to Dakar, the NAO was only provided with a copy of the '*Dakar Payroll Software Maintenance*' agreement and ensuing correspondence, available in the MDH file. No further SLAs concerning the MDH Dakar software application, if existent, were made available.

The undated agreement was endorsed by both parties in December 2004, although neither the duration, nor the exact start or end dates were clearly stipulated. The agreement does however states that the "*termination may be requested...at least 3 months prior to the due date of annual renewal*", implying that the agreement is automatically renewable annually.

The agreement, which quotes rates in Maltese Lira (*Lm*), specifies an annual maintenance fee for '*Dakar Payroll, Personnel and Rostering systems*', plus an additional fee for on-site visits, including bug-fixing. The agreement further states that "*the terms of this agreement cannot be changed unless agreed to and signed by both parties...*" whereas another clause states that "*the rates and charges in the maintenance agreement may change from time to time*", without specifying when they may be changed, by how much, or the procedure for informing and approving such changes from the MDH side. To this effect, the NAO noted that the supplier increased the rates at least once, by 25%, with effect from January 2009.

Additionally, the NAO noted that in April 2004, the supplier had already quoted the same terms, conditions and fees, whilst providing a specimen software maintenance agreement, following a meeting held between both parties. Moreover, the NAO observed that over the years, MDH has sought to obtain Direct Order approvals from both the Ministry of Finance and the Department of Contracts on various occasions, concerning 'software support fees' (on-site support visits) and 'annual licensing fees' for Dakar. In fact, approvals were obtained on at least seven separate occasions, covering the period 2005 to 2015, and cumulatively amounting to over €255,000 (inclusive of VAT).

2.8 Network Infrastructure

A network infrastructure refers to the hardware and software resources of an entire network that enables network connectivity, communication, operations and the management of an enterprise network. It mainly includes switches, routers, wireless routers, cabling, firewalls, network security applications, IP addressing, wireless protocols etc. Thus, a network infrastructure can be considered as the communication path between users, processes, applications, services and external networks.

In 2005, FMS entrusted MITA for the design, implementation and management of the entire network infrastructure at MDH, which is based on the classic hierarchical topology that collectively provides for redundancy, security, performance and scalability.

Taking into consideration the criticality of MDH in the provision of effective and efficient, acute patient-centred quality care, the elimination of service downtime is the most important element of the whole MDH network infrastructure. As a result, the MDH network infrastructure has multi-gigabit links operating in full-duplex mode, to avoid issues with network collisions and to provide full bandwidth in both directions simultaneously. Furthermore, the MDH network has multiple paths and links available to any given destination. This plays a vital role when it comes to load distribution, since this mechanism determines the flow of traffic, and therefore the efficient use of resources, within the MDH network.

In terms of security, the MDH network infrastructure consists of two high-performance security appliances that determine the incoming and outgoing network traffic flow. These security appliances operate on an active/passive cluster, whereby an identical passive appliance backs up the active appliance.

Finally, due to its modular design the MDH network infrastructure has been designed to address future growth, in terms of capacity, size and structure. However, since the long-term business requirements were virtually unknown at the design process, various options were taken into consideration in terms of the network scalability, in the context of the MDH network topology.

With reference to the LAN infrastructure, the NAO was informed that the MDH network is logically segmented into a number of Virtual LANs (VLANs). The latter logically separates and isolates certain traffic from other traffic on the network, whether it is data, voice or other. In this regard, VLANs offer a number of benefits in terms of security, cost reduction, better performance, improved IT staff efficiency and simpler project and application management amongst others.

During the course of the IT audit, the NAO was informed that the MDH network, which is connected to the MAGNET via fibre-optic links to both MITA's Government Corporate Data Centres in St. Venera and MDH, is monitored and maintained by MITA on a 24/7 basis as part of the MITA core services contract. Furthermore, MITA also maintains all the network hardware, including the routers and switches installed across MDH, and provides the necessary support on the WAN and LAN infrastructures.

Whilst reviewing the MDH network setup, the NAO was informed that MDH has around 30 network cabinets of which two are solely managed and accessed by MITA. The remaining 28 network cabinets are managed by MITA, but the IT Technical Support team can also access these network cabinets whenever they need to patch network points and connect any IT equipment to the MDH network. The NAO observed that the network rooms where every cabinet is installed are secured under lock and key, and the IT Technical Support team must sign for the key whenever they need to access a particular network room. During the course of the IT audit, the IT Technical Support team provided the NAO access to some of these network rooms. In this regard, the NAO observed that overall the network rooms are very well kept, whereby every room is kept free from clutter and equipped with an air-conditioning unit, which is monitored and maintained by the Engineering department within MDH. Furthermore, most of the network cabinets are properly labelled and the cabling is well organised, whilst the networking equipment is connected to an Uninterrupted Power Supply (UPS). In the event of a hardware malfunction, both the UPSs and the networking equipment are maintained by MITA.

In the meantime, the NAO is pleased to note that access to the MDH LAN is restricted with network port locking. Thus, when connecting a new workstation or moving an existing workstation from one point to another, the IT Technical Support team must raise a service request with MITA's Service Call Centre to ensure that the network connectivity is available. If the network connectivity is not available, then either the same request is escalated to the relevant Service Team or another service request is raised specifically for the issues encountered.

Finally, the NAO was informed that apart from the network connectivity to the MAGNET, MDH has a third party Wi-Fi connection at the Administration section, which is only accessible by the CEO and

the respective Directors within this section. If an individual requires access to this Wi-Fi connection, a business case must be submitted to the respective Directors and access is only granted at their discretion. The NAO was informed that this third party Wi-Fi connection was configured by the Networks team, according to MITA's standards, and the password is securely kept and changed regularly. At the time of the audit, the NAO was informed that the Networks team were liaising with MITA to replace the current third party Wi-Fi connection with a Wi-Fi connection provided by MITA.

In the meantime, the NAO was also informed that apart from this third party Wi-Fi connection at the Administration section, MDH has a number of Wi-Fi connections throughout MDH, which do not fall under the responsibility of the IM&T unit. These Wi-Fi connections are managed and maintained by the respective third party service provider and are segregated from the MDH network infrastructure.

Chapter 3

IT Applications

Chapter 3

IT Applications

3.1 Access Dimensions

The Access Dimensions application was first launched when St Luke's hospital (SLH) was Malta's main general hospital before MDH became the public hospital in Malta in 2007. The Access Dimensions application is an off-the-shelf software application that is mainly used to control stock movements, including the recording of items upon receipt and invoicing for items upon issue from four different areas, namely SAMOC, the Pharmacy department, the Finance department and the MM&L department within MDH.

The Access Dimensions application has a Microsoft SQL database with two instances. One instance that caters for SAMOC, and the Pharmacy, Stores and MM&L departments within MDH, resides on a dedicated Microsoft Windows 2000 server, whilst the other instance, used by the Finance department, resides at MITA's SHE. With regards to the first instance, although MDH is aware that the Microsoft Windows 2000 server is obsolete and no longer supported by Microsoft, the server hardware is quite old and thus has its limitations. The NAO is of the opinion that the above-mentioned server is decommissioned and the SQL database is migrated on a virtual environment and hosted at MITA's SHE. In this regard, the NAO was informed that discussions are currently underway with MITA on the possibility of migrating the current setup to Microsoft Windows server 2012 and hosting it on MITA's SHE.

At the time of the IT audit, the Access Dimensions application was being maintained by one ICT Application officer within the IM&T unit, in terms of account management and to provide first line technical support to the end users within MDH when required. Furthermore, this ICT Application officer also liaises between the local third party supplier and MITA whenever any enhancements, software upgrades or technical assistance is required. The NAO was informed that at the time of the IT audit, the ICT Application officer only had access to the SQL instance hosted on the Microsoft Windows 2000 server, whilst the local third party supplier had elevated privileges to access the SQL instance residing at MITA's SHE through a secure Virtual Private Network (VPN) connection.

Furthermore, the NAO observed that at the time of the IT audit, MDH did not have any written SLAs with the local third party supplier, and when MDH requires the assistance of the local third party supplier, the latter provides a service on a time and material basis. However, the NAO was informed that MDH together with the Ministry's IMU (Health) were in the process of finalising an SLA with the local third party supplier, which should have been concluded by the end of Q4 2015.

Whilst reviewing the Access Dimensions application in terms of user account management, the NAO was informed that whenever a new user wishes to gain access to the Access Dimensions application, their respective Head of department must send an e-mail request to the ICT Application officer. In turn, the ICT Application officer will forward the request to MITA's Service Call Centre, to raise an incident request for the creation of a new user account. The incident request is then escalated to the ICT Application officer for the creation, modification or deletion of user accounts or to assign user roles. In this regard, the NAO observed that the *'user id's* are created haphazardly, in the sense that the *'user id's* do not follow a standard naming convention. In this regard, the NAO is of the opinion that the ICT Application office together with the local third party supplier should review the *'user records'* table, and ascertain that the *'user id's* and the *'name'* fields follow a standard naming convention which is easily identifiable.

Furthermore, the NAO observed that the Access Dimensions application does not offer any password security controls, in terms of password complexity, password expiry, password history or a mechanism whereby the user is forced to change his/her password upon first logon. The NAO recommends that the ICT Application officer should liaise with the local third party supplier and establish whether the Access Dimensions application can be enhanced in terms of password security controls.

In the event that a user has forgotten his/her password, the user must send his/her request to the ICT Application officer through the Government e-mail. In turn, the ICT Application officer raises an incident request with MITA's Service Call Centre. Similarly, the incident request is escalated to the local third party supplier since the ICT Application officer does not have sufficient user privileges to change passwords. When a new password is generated, the local third party supplier sends the new password by e-mail to the user's mailbox. In addition, the NAO was informed that whenever a user retires or no longer requires access to the system, the user account is disabled only if the ICT Application officer is informed by the respective Head of department through the Government e-mail. The same procedure applies for users who are on prolonged leave, career break or maternity leave. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all the staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit is informed accordingly, and the respective user accounts are disabled.

The NAO was informed that the Access Dimensions has an audit trail in place for any failed or successful user login attempts, which are only accessible by the local third party supplier at the backend, since the ICT Applications officer does not have sufficient user privileges to view these logs.

During the course of the IT audit, the NAO interviewed a number of users and observed how they maintain stock items on the Access Dimensions application. In this regard, the NAO was informed that stock items are organised and stored in different locations, namely:

- MDH Stores (former Madliena Stores) – where medical devices and fast-moving items, such as disposable syringes or swabs etc. are kept;

- General Stores in G'Mangia – where provisions, such as cleaning and stationery items are kept; and

- San Gwann Stores – this is the main Health depot, whereby most disposables, pharmaceutical, conjoints[4] and special items are kept.

With the exception of the San Gwann Stores, which uses a SAGE application, the MDH Stores and General Stores in G'Mangia utilise the Access Dimensions application for their stock items. Notwithstanding the above, both the SAGE application and the Access Dimensions application have an identical system for stock item codes. However, prior to April 2011, the Access Dimensions application had different stock item codes before these were replaced with newer codes to reflect the stock item codes that exist in the SAGE application. Even though the previous stock item codes still exist on the Access Dimensions application, these are no longer used but are solely being kept as a point of reference to previous transactions.

The NAO was informed that in the event of a defective or damaged stock item, these are forwarded to the MM&L department within MDH. In this scenario, the department would raise an incident report and inform the respective supplier or agent through an e-mail, whilst keeping the Malta Competition and Consumer Affairs Authority in the loop. Each stock item is investigated and quite often, the respective agent or supplier would provide an identical replacement. In more complex situations, the MM&L department might involve the Malta Standards Authority, who in turn would investigate the case from a technical/scientific perspective. In extreme cases, if the supplier or agent does not accept responsibility, the MDH would then seek the assistance of a lawyer.

The NAO observed that the Access Dimensions application offers a number of pre-defined Crystal reports although only around 15 reports are generally used. Whilst reviewing the reporting functionality, the NAO observed that the end user can execute a specific report to check which stock items are not in stock, and could also execute a different report that indicates which stock items are running low in stock. The NAO recommends that such reports are automated or better still the system should incorporate an alerting mechanism that automatically notifies the persons in charge whenever essential stock items are running low in stock.

Furthermore, when generating a report on the number of stock items consumed during a given period in a particular ward or clinical area, such reports are generated repetitively to cater for every ward or clinical area within MDH. These reports are then exported on to Microsoft Excel so that the user could easily analyse, filter and process all the data compiled from the report. At the end of the year,

[4] Conjoints are stock items of disposable nature used mainly in wards or clinical areas within MDH

such reports are very useful for the Supplies department when reviewing the number of stock items consumed in every ward or clinical area, to determine the expected consumption for the forthcoming year and set quotas for every ward or clinical area within MDH. The NAO observed that apart from the number of stock items and the total cost of all the stock items consumed over a given period in a particular ward or clinical area, the report does not include the cost of every stock item. Thus, the user cannot quantify how much each stock item costs. At the time of the IT audit, whenever an itemised report was being requested, every stock item was being calculated manually in Microsoft Excel to determine the actual cost. The NAO recommends that an itemised report that would include the cost for every stock item rather than just the total cost of all the stock items consumed is made available to a restricted number of authorised users only.

3.2 Centricity Picture Archiving and Communication System and Centricity Radiology Information System

The Centricity Picture Archiving and Communication System (PACS) is an off-the-shelf software application for managing digital medical images and associated data. It utilises a standard-based, customisable and scalable solution supporting the Integrating the Healthcare Enterprise (IHE) profiles, Digital Imaging and Communications in Medicine (DICOM), and the Health Level Seven (HL7) protocol standards for the handling, storing, printing and transmitting of digital medical images and patient data.

In this regard, the Centricity PACS is used to acquire, archive, and view digital images and data from diagnostic imaging devices such as PET-CT scans, Digital Mammography, Magnetic Resonance, Ultrasound, X-rays etc. that are then sent to the PACS application and stored in a database. The system, which is integrated with the Centricity Radiology Information System (RIS) application, is mainly used by Doctors, Speech Language Pathologists, Physiotherapists, Podologists, Radiographers, Specialised nurses and Dentists within MDH, GGH, SAMOC, Karin Grech Rehabilitation Hospital, the Breast Screening Centre in Valletta, and a number of Health Centres across the Maltese islands. Furthermore, the Centricity PACS application is also integrated with the CPAS application to retrieve patient demographics.

On the other hand, the Centricity RIS is an off-the-shelf web-based radiology information system designed to address the evolving radiology workflow needs and is thus considered as the backbone software application for the workflow in the Medical Imaging department within MDH. Apart from the Medical Imaging department, the Centricity RIS is also used at the Cardiology, Gynaecology and Dental departments within MDH, and at GGH, SAMOC, the Breast Screening Centre in Valletta and a number of Health Centres across the Maltese islands.

The Centricity RIS, which is also integrated with the Centricity PACS and the CPAS application to retrieve patient demographics, handles the scheduling of patients, including the printing of appointments, the reporting of examinations by Radiologists, the management of user accounts and auditing. The Centricity RIS application provides the functionality for extracting statistical data and provides the Radiology modalities (such as CT scans, Ultrasound etc.) with a patient work-list that automatically updates the RIS database once a patient's examination is completed.

At the time of the IT audit, both the Centricity PACS and RIS applications were hosted on active/passive Microsoft Windows servers at MITA's Data Centre at MDH and at MITA-01 Data Centre in St. Venera. As part of MITA's Hosting Services Contract, MITA is responsible for the hosting and monitoring of servers in terms of hardware and network infrastructure and the monitoring of the backup process. In this regard, both the Centricity PACS and RIS servers were configured with the *'grandfather-father-son'* backup rotation, whereby an incremental backup to disk is scheduled on a daily basis, whilst a full system backup is scheduled weekly or monthly and stored on MITA's storage environment. In the event that a backup process fails to complete, the Network Operations Centre within MITA will inform the MITA Health team accordingly. Meanwhile, to ensure that the data can be fully restored from the backup files, the NAO was informed that MITA carries out a random test restore from the pool of backup files every quarter.

The NAO was informed that a new PACS/RIS hardware and software maintenance contract was signed between MEH and the third party supplier for the provision of hardware and software maintenance and support. Furthermore, the NAO observed that the service contract stipulates that the Microsoft Windows servers will be replaced, in terms of hardware and operating system, whilst the PACS application is upgraded from version 3.0 to version 4.0, and the RIS application is upgraded from version 4.2 to version 5.0. Furthermore, the high-resolution screens and the workstations at the Medical Imaging department will be replaced and installed with the latest software release. In this regard, the NAO was informed that whilst the Microsoft Windows servers and applications were replaced or upgraded by Q2 2015, at the time of the IT audit most of the high-resolution screens were in the process of being replaced.

The NAO was informed that these high-resolution screens are specifically approved for medical diagnosis. As a result, these screens have a built-in stabilisation and patented front-of-screen sensors that guarantee consistent image brightness and clarity throughout the entire display lifespan. Furthermore, these screens are connected to the Government network so that the third party supplier could monitor these high-resolution screens remotely and run daily checks on the screen's brightness and uniformity.

During the course of the IT audit, the NAO interviewed key stakeholders and observed how the Centricity PACS and RIS applications are being maintained, in terms of account management, system health checks, management reports, backups, user training and the updating of the hardware and software inventory amongst others. In this regard, the NAO observed that both systems are maintained by an ICT Manager, in the role of a System administrator, and is assisted by the MITA Health team and the third party supplier, who provide second and third line support respectively, according to the established SLAs. In the absence of the ICT Manager, specific users within every section or department were granted elevated privileges to administer user accounts, manage the PACS generic mailbox or to monitor the RIS user licences.

Whilst the ICT Manager has administrative access privileges to maintain the Centricity PACS and RIS applications, the NAO was informed that only the third party supplier owns the local administrator password. The latter is used to gain remote access on the Centricity PACS and the RIS servers, through a secure VPN connection, to provide technical assistance or to carry out the necessary software enhancements and upgrades, according to the established change management procedures.

If a new software enhancement or upgrade is implemented by the third party supplier, the latter will provide adequate training to key stakeholders within the MITA Health team and the ICT Manager. This kind of training would normally include training on new features, assistance on the Centricity PACS and RIS downtime procedures definition and testing, and the use of the Centricity PACS and RIS administrative tools. The ICT Manager would then adopt the train-the-trainer approach to a number of specific users within every section or department, who in turn would train the remaining users within their respective section or department.

Whenever a new user wishes to gain access to the PACS or RIS application, a *'Request for IT Service form'* is filled-in and signed by the relevant stakeholders. These forms are handed in to the IT Support Services team within the IM&T unit to raise the necessary eRFS with MITA. In turn, MITA will raise an incident request for the creation of a user account on PACS or RIS, and since the PACS and RIS servers are members of the CORP Domain, the user's CORP Domain account is added to the respective PACS or RIS user groups in the Active Directory. The incident request is then escalated to the ICT Manager for the creation of a user account on the PACS or RIS application. At the time of the IT audit, the NAO observed that the Centricity PACS application had 3,157 user accounts, whilst the Centricity RIS application has 620 user accounts.

Upon creation of a user account, the ICT Manager will assign the user privileges according to their role within their respective section or department. In this regard, the NAO was informed that the Centricity RIS application offers only two different user levels, in which user accounts can be granted either administratively or through user level access privileges. On the other hand, the Centricity PACS has different user levels, which are sorted into groups. Thus, a user account can be linked to either the MITA group, the PACS administration groups, the References Group or the Browsing group and according to one's speciality.

The NAO observed that whenever a new user account is created, the password is set with a minimum number of characters and the user must change password upon first logon. Furthermore, the system will block the user after a number of unsuccessful login attempts in which case only the ICT Manager can unlock the user account. Even though passwords are encrypted, currently the system does not have any password security controls in terms of password complexity or password history. In addition, user passwords were configured to expire between three to five years rather than over a stipulated number of days. In the meantime, the NAO is of the opinion that the ICT Manager and all the relevant stakeholders should look into the possibility of enhancing the password security controls on both the Centricity PACS and RIS applications.

In the event that a user has forgotten his/her password, the user is requested to phone MITA's Service Call Centre, whereby an incident request is raised. If the user requests a new password to access the Centricity PACS application, a new password is generated by MITA and sent to the user's Government e-mail. Alternatively, if the user requests a new password to access the Centricity RIS application, MITA will forward the request to the application's generic mailbox, whereby either the ICT Manager or the specific users within the section or department, can reset and generate a new password or unlock a user account through the Centricity RIS administrative tool.

The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is only disabled if the ICT Manager is informed through the Government e-mail. A similar procedure is applied for users who are on prolonged leave, career break or maternity leave, whereby the user account is disabled until the user returns to work. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed accordingly, and the respective user accounts are disabled or deleted accordingly.

Furthermore, the NAO was informed that user accounts cannot be modified or deleted, but they are de-activated and can be used for future audits. In this regard, the NAO observed that both the Centricity PACS and RIS applications offer a number of in-built audit queries, whereby the ICT Manager, through the PACS or RIS administrative tool, can extract the required audit logs, which can be then exported and filtered in a Microsoft Excel worksheet.

Finally, whilst reviewing the Centricity PACS application, the NAO was informed that whilst most of the workstations and high-resolution screens were being replaced, the CD Robotics equipment at the Medical Imaging department could not be connected to the new workstations as they are only compatible with the Microsoft Windows XP operating system. Since the latter is no longer supported by Microsoft and MITA, it is envisaged that the third party supplier will start replacing the CD Robotics equipment in Q1 2016 as stipulated in the new hardware maintenance contract. At the time of the IT audit, the Medical Imaging department only had a few remaining workstations installed with the Microsoft Windows XP operating system to operate the CD Robotics equipment until the third party supplier replaces them.

In addition, since the RIS application can only be accessed if the application is installed on specific workstations, whenever a new RIS installation is required, an incident request is raised with MITA's Service Call Centre. However, the NAO was verbally informed that there were instances in the past whereby the RIS application was installed on workstations without the ICT Manager's consent, when the latter was unavailable. This contributed to the further saturation of user licenses and the hardware and software inventory not being updated. In this regard, the NAO is of the opinion that RIS installations should always be approved by the ICT Manager to ensure that such installations are kept under control. In the meantime, if the RIS application has reached the limit of the number of concurrent user licences and users cannot log on to the RIS application, the ICT Manager can end the user sessions, which have been inactive for the longest period of time. The NAO was informed that to lessen the burden of the saturation of user licenses, additional user licences were added in Q1 2015, as part of the new hardware and software maintenance contract.

3.3 Clinical Patient Administration System

The Clinical Patient Administration System (CPAS) application, which was developed in-house, is the backbone application of all Health systems and was launched in 2013, to replace the old Patient Administration System (PAS). The aim of the CPAS application is to store the main patient master index and episode tracking, inpatient and outpatient appointments, the Nurses' time-off-in-lieu and various other modules. As highlighted earlier in the report, the CPAS application provides patient demographics to a number of critical applications, such as iCM, CVIS, LIS, RIS and PACS, and is used

across the various Health entities, including MDH, SAMOC, GGH, MCH, and Karin Grech Rehabilitation Hospital, Health Centres, SVPR, Dar il-Kenn and Mtarfa home.

At the time of the IT audit, the CPAS application was hosted on two Microsoft Windows Clustered servers, which were situated at MITA's MDH Data Centre. As part of the hosting services contract, MITA is only responsible for the monitoring of the network connectivity and the loading/unloading and storage of the backup media on a daily basis. On the other hand, the CPAS hardware, software application and system backups were being monitored and maintained by a local third party supplier. Thus, in the event that a daily/weekly/monthly backup fails to complete, MITA will inform the local third party supplier through an e-mail, whilst the Director Health Informatics is kept in copy. Similarly, when a backup has been successfully completed, an e-mail notification is automatically sent to the Director Health Informatics and the local third party supplier respectively.

In addition, the old PAS server is still running and is hosted at MITA's MDH Data Centre. However, the NAO was informed that the previous PAS application can only be accessed to view past records and is not being kept in sync with the current CPAS application. When the CPAS application was launched in 2013, only some data, such as patient demographics and future appointments, was migrated from the previous PAS application. At the time of the IT audit, MDH did not intend to switch off the PAS server unless all the data residing on it was completely extracted and presented in a readable format. In this regard, MDH held a number of discussions on the possibility of extracting such a large amount of data from the old system, filter all the data and try to match all the tables of the old system with the tables of the new system. The NAO was informed that even though MDH had approached local third party suppliers, no one is willing to take the risk in doing this laborious task. In this regard, MDH are looking into other possibilities of extracting data, which may involve foreign third party suppliers.

As highlighted earlier in the report, MDH has a dedicated team that offers first-line technical support to all the end users at MDH and other entities who have been granted access to the CPAS application. The CPAS team, which is made up of a clerk acting as a System administrator and two sub-contracted clerks responsible for the overall administration of the system. This includes the management of user accounts and user roles, the management of the outpatient booking system, performing system testing whenever a new functionality is added to the CPAS application and the organisation of user training from time-to-time and as necessary.

The CPAS team also offers a Helpdesk functionality within MDH during office hours, whereby the end users can phone directly whenever assistance is required. However, the NAO was informed that the end users are instructed to phone MITA's Service Call Centre whenever any issues on CPAS are encountered, since the CPAS team does not have any traceability on the number of calls that are being handled through the Helpdesk function. In this scenario, whenever an end user phones MITA's Service Call Centre, an incident request is raised in MITA's Call Logging system and is then escalated to the CPAS team, who would service the request accordingly.

With reference to user training, apart from the IT Trainers within the IM&T unit, who offer user training to new recruits, the CPAS team also offers one-to-one training to the end users. This is often the case when a new functionality has been added in CPAS to cater for a particular ward or department. For instance, at the time of the IT audit, the CPAS team delivered specific training to a number of users at

SAMOC after a new functionality was added on CPAS. In addition, the NAO was informed that in 2015, the CPAS team started offering refresher courses across the wards to a number of users who requested training. In this regard, the CPAS team tries to allocate one-to-one training sessions of one-hour duration twice a day during office hours. Furthermore, the NAO was informed that before the CPAS application was launched in 2013, a number of training sessions were offered to all the prospective CPAS users within the Health entities. However, the NAO observed that certain users interviewed during the course of the IT audit, were not confident in using certain functions of the CPAS application and sometimes get confused on how to carry out a particular function. Whilst the NAO commends all the effort being put through by the CPAS team, in offering refresher courses, more effort is required so that the end users are made aware that such courses are held and that they should contact the CPAS team if refresher or specialised courses are required.

Apart from the CPAS team, the system is also maintained by two different local third party suppliers offering database support on a 24/7 basis and carrying out system development as needed. At the time of the IT audit, the NAO was informed that MDH had renewed the supplier maintenance contract with the System developer for the next three years, whilst the supplier maintenance contract for database support was being finalised. In the meantime, MDH has a separate hardware maintenance contract for both CPAS servers. Whilst the current hardware maintenance contract stipulated that the local supplier would offer a service on a time and material basis, MDH had submitted a request for quotation to the local supplier for the provision of 24/7 hardware maintenance contract for both CPAS servers for the next three years.

The NAO was informed that whenever a change or a new functionality is required on CPAS, the users are requested to submit an e-mail, which must be endorsed by their superiors, and clearly state why this is required. These requests are then vetted by the CPAS System administrator and the Director Health Informatics, and prioritised according to their business requirements. Once these requests are grouped and prioritised accordingly, the CPAS System administrator and the Director Health Informatics would then discuss these changes together with the section/area that initially raised the requests. However, if a change or a new functionality in the system is required to reflect a new legislation, this would be given higher priority above the rest. Prior to these changes being developed, weekly meetings are held with the CPAS System administrator, the Director Health Informatics and the System developer to discuss the changes or new functionalities that are required on CPAS. Once these changes or functionalities are developed, they are uploaded and tested on the CPAS testing environment, before they are implemented on the *'live'* environment. In this regard, the NAO is pleased to note that the CPAS team has been documenting all these user requests in a Microsoft Excel worksheet. The latter include the date when the end user has forwarded the request, whether the request was forwarded to the System developer for implementation and the feedback provided by the System developer showing whether the change has been completed. In addition, the NAO was informed that every change or functionality that is added on to CPAS is being documented and conforms to the Change Management procedures via MITA's Service Call Centre.

Whilst reviewing the CPAS application in terms of the management of user accounts, the NAO observed that whenever a new user wishes to gain access to the CPAS application, a *'Request for IT Service form'* is filled-in and signed by the relevant stakeholders. Similarly, whenever a number of users are employed within MEH and require access to the CPAS application, the Directorate to whom

these individuals would report to and the HR section within MDH, would liaise with the CPAS team and forward all the relevant details in a batch. All the forms are handed in to the IT Support Services team within the IM&T unit to raise the necessary eRFS with MITA. Since MITA does not have access to manage user accounts, MITA would raise an incident request for the creation of a user account and escalate the incident request to the CPAS team. The latter would then create a user account on CPAS and grant access rights so that users could view only, admit patients in wards, or admit/register patients at the Outpatients department, amongst others.

The NAO observed that whenever a user account is created, the CPAS application does not adhere to password management best practices. The system does not offer any password security controls in terms of password complexity, password expiry, and password history, or block the user after a number of unsuccessful login attempts.

Furthermore, in the event that a user has forgotten his/her password, the user is requested to phone MITA's Service Call Centre, whereby an incident request is raised and escalated to the CPAS team. The latter would then change the user account password and the new password is sent to the user on to his/her Government mailbox. In this scenario, the NAO observed that when a new password is sent to the user, the CPAS application does not prompt the user to change password upon first logon. Thus, since the system does not have any password security controls in place, most of the user account passwords are never changed. In this regard, the NAO is of the opinion that MDH should look into the possibility of enhancing the password security controls on CPAS and adopt password management best practices.

The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is disabled only if the CPAS team are informed through the Government e-mail. A similar procedure is applied for users who are on prolonged leave, career break or maternity leave, whereby the user account is disabled until the user returns to work. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed, and the respective user accounts are disabled or deleted accordingly.

At the time of the IT audit, the NAO was informed that on implementation, the CPAS application had a tracking system, that recorded the date and time when a user logged on to CPAS, searched for a patient or viewed a patient's clinical episodes amongst others. However, since the tracking system was generating a large amount of audit logs, which was impacting the performance of the CPAS server, the CPAS team were instructed to disable this tracking functionality from the front-end. Nonetheless, the NAO was informed that the tracking functionality is still running at the back-end to record all the events. Thus, in the event that senior Management requests to view the audit logs of a user at a particular point in time, the CPAS team must inform the database support local third party supplier to extract the logs and provide the requested information. To overcome this problem, the NAO was informed that a request for quotation was sent to a local supplier for the upgrading of the CPAS server. In this regard, it is envisaged that when the CPAS server is upgraded, the tracking system is fine-tuned and will be accessible again from the front-end to a limited number of users for investigative purposes.

During the course of the IT audit, the NAO interviewed and observed a number of key users within MDH on the use of the CPAS application, in terms of how they update patient details, schedule new appointments, register patients, update patient visits and generate reports from CPAS.

In this regard, whenever a patient walks in at MDH for an appointment at the Outpatients department or to be admitted for a medical/surgical intervention, the end users are instructed to verify the patient's personal details and ensure that all the necessary details are correct. However, at the time of the IT audit, the NAO observed that users from different departments raised a number of issues, when updating the *'Patient Interface'* module on CPAS, including:

- When inputting a patient's e-mail address, the CPAS application was prompting the end user with an error statement, informing that the e-mail address is invalid and must contain the symbol *'@',* even though the end user had typed in a valid e-mail address according to the required syntax. Prior to this, end users used to type in comments in the e-mail address field, since a comments field does not exist, before a rule was implied on this field to include the *'@'* symbol and a limited number of characters.

- The NAO was informed that as an internal procedure, an adult should always accompany a patient under 18 years of age. However, there are instances whereby the *'Age'* field is blank and not calculated automatically even though the patient's date of birth was inputted correctly. This may lead to a situation where the user cannot determine at a glance whether the patient is under age and should be accompanied by an adult. In this regard, the CPAS team informed the NAO that the patient's age is calculated automatically as long as the end user clicks on the blank *'Age'* field.

- Similarly, there are instances whereby the patient's date of birth is unknown. This is mostly attributed to foreigners, whereby the date of birth is registered by default to 1st January 1900.

- Finally, deceased patients are flagged in CPAS and the patient's details are highlighted in green. However, the NAO was verbally informed that there were instances whereby deceased patients were not flagged in a timely manner on CPAS and clinical appointments that were already re-scheduled, were still sent to the deceased person by post. In this scenario, end users felt embarrassed when a relative phones at MDH to cancel the appointment since the patient had passed away days or weeks ago.

Taking into consideration that the CPAS application provides patient demographics to a number of critical applications within MDH, the NAO recommends that MDH should continuously emphasise on the importance of updating the patient demographics and ensure that the end users are aware of how to update the necessary fields.

In this regard, the CPAS team informed the NAO that the *'Patient Interface'* would be revamped and most of the above issues will be taken into consideration in the next CPAS enhancement scheduled for Q4 2015. For instance, the current *'Age'* field does not calculate the age of children less than a year old. It is envisaged that the new *'Patient Interface'* will calculate the age of newborns or children less than one year old in days, weeks or months.

In the meantime, the NAO observed that every Consultant has his/her own clinic and each clinic is identified on CPAS with a clinical code. Thus, when scheduling an appointment, the end user can check for any available slots from the CPAS calendar and register the patient's new appointment as *'new', 'follow-up'* or *'investigation'*. The NAO was informed that the slots allocated in CPAS are defined by the respective Consultant and approved by the Medical administrator. In this regard, the Consultant and the Assisting Nurse can view the available slots, the number of appointments scheduled on a particular day, whether there is an overbooking on a particular date/clinic and can also view the priority slots. The latter are normally allocated whenever a Consultant needs to examine a patient within three or four days after the patient underwent a medical or surgical intervention.

Whilst reviewing the CPAS application, the NAO observed that when setting up an appointment, the system does not prompt an error or warning if the patient already has an appointment scheduled on that date. Having said that, upon searching for a patient through their ID card number, the end user can view the previous and future clinical appointments registered on CPAS in the *'Episodes Area',* however these are not listed chronologically. In this regard, the NAO recommends that the *'Episodes Area'* is refined to list the previous and future clinical appointments chronologically, whilst the past clinical appointments are easily identified from the rest, whereby these may be either greyed out or else displayed in a different font or colour.

In addition, the NAO observed that certain users are having difficulties finding available slots allocated in a particular clinic, when setting up an appointment. This is due to the fact that some clinics are overloaded with patient appointments especially at the outpatient's department. If a Consultant requests that a particular patient is admitted to MDH for a follow-up on a particular date but the slots available on CPAS are all booked, the Clinical Nurse assisting the respective Consultant has to phone the CPAS team every time a new slot needs to be added on a particular clinic. In this scenario, there are instances, especially on a Saturday, whereby the Clinical Nurse at the Outpatient's department must wait until Monday to book a patient appointment on CPAS, because the CPAS team can only be reached from Monday to Friday, during office hours, to allocate new slots to a particular clinic on a specific date. In this regard, the NAO was informed that Clinical Nurses, assisting the respective Consultant, used to have this functionality when using the previous PAS application. However, when the CPAS application was implemented in 2013, this functionality was no longer available and thus the Clinical Nurses have to contact the CPAS team every time they need to add new slots. In view of this, the NAO recommends that MDH should look into this matter and evaluate whether elevated privileges can be assigned to specific users so that they can allocate new slots to a particular clinic when applicable.

On the other hand, if a Consultant or a Doctor needs to a cancel all the appointments scheduled on a particular date, the Clinical Nurse assisting the respective Consultant or Doctor cannot cancel and reschedule any patient's appointments unless they receive a written approval from higher officials through the Government e-mail. Once the request is approved, the Clinical Nurse can proceed with the cancellation and rescheduling of appointments at a later date. In this regard, the NAO observed that the system does not offer the functionality to cancel and reschedule the appointment scheduled on that particular date in bulk but has to cancel and reschedule every patient's appointment one-by-one. Once all the appointments have been cancelled and re-scheduled at a later date, the Clinical Nurse must inform the CPAS team through the Government e-mail to block the date from CPAS to ensure that no clinical appointments are booked under that particular Consultant or Doctor on that day.

In the meantime, whenever an appointment is cancelled, the patient is informed over the phone that the scheduled appointment has been cancelled and rescheduled at a later date. If the patient could not be reached, the patient is informed in writing by post. The NAO observed that when the end user is about to cancel an appointment, the user is prompted whether to print the cancellation of appointment or not. In this regard, if the end user refrains from printing the cancellation of appointment, the CPAS application will not allow the user to print the cancellation of appointment letter at a later stage. The same applies if the printer malfunctions when it is supposed to print the cancellation of an appointment letter. In this scenario, the end user has to print the original appointment letter and make a note that the appointment has been cancelled. When the new appointment is rescheduled, the end user would print the new appointment letter, attach it to the cancellation of appointment letter and send these to the patient by post. In this scenario, the NAO recommends that the user is given the option to print the cancellation of an appointment letter again or the cancellation of an appointment letter and the new appointment letter are grouped and printed on the same letter. Furthermore, the NAO also recommends that such notifications are sent through SMS or e-mail.

The NAO observed that whenever a foreign patient walks-in for an appointment or treatment at MDH, the end user would inform the patient to visit the Billing section within MDH before the end user could register the patient in CPAS. The Billing section would check whether the patient is a UK resident or married to a Maltese citizen. If this is the case, the Billing section would flag the patient on CPAS such that no costs would be incurred, whilst other patients would be flagged in CPAS such that a cost would be incurred according to the treatment received at MDH. At the time of the audit, whenever a foreign patient walks-in for an appointment or treatment at MDH, the CPAS application did not offer the functionality to automatically trigger a notification to the end user on whether the patient would incur any charges or not. In this regard, the NAO was informed that it is envisaged that this feature may be included when the *'Patient Interface'* is revamped in the next CPAS enhancement scheduled for Q4 2015.

In addition, when a patient is discharged from MDH, the end user must update the patient details and mark the patient as discharged to be reflected in the CPAS patient history file. However, since the discharge letter is issued from the ECS application, the NAO recommends that MDH assess whether the ECS application is integrated with CPAS. Thus, once a patient is marked as discharged, the end user could either open an ECS session through CPAS or else view the patient's discharge letter from CPAS once it has been compiled on the ECS application.

During the course of the IT audit, the NAO was informed that the *'live'* data on CPAS is being backed up on the hour on a different server, so that users could easily generate custom-made reports from this server through a specific reporting tool, without impacting users on the *'live'* environment especially when extracting statistical reports. On the other hand, the NAO observed that the CPAS application has a reporting functionality whereby a number of standard reports can be generated according to the level of access and location assigned to the end user. Thus, the reporting menu on CPAS includes:

- **Bed Status Report** – this report is mainly used by the end users who are assigned to a particular ward and the Bed Management unit within MDH, whereby they can view the number of occupied and unoccupied beds available in every ward. The report can be either displayed on screen or extracted and saved in *'.csv'* format.

- **Episodes/Ticket Report** – this report is mainly used at the Outpatients department, whereby end users who are assigned to this department can view the number of clinical appointments scheduled on a particular day/s in a particular clinic. This report would include the patient ID card number, patient's name and surname, the appointment type (whether it is a new case, follow-up or investigation), ticket ID, the total number of appointments scheduled on that particular date, and may also include the patient's phone number or if an appointment has been cancelled.

- **Event Report** – this report can be used at the Inpatients and Outpatients wards/clinics, whereby users can gather data of any type of events as registered in CPAS, for instance, patient admissions on a particular date in a particular ward, clinic or hospital.

- **Transport Report** – this report is mainly used to lists patients who booked for transport and the total number of patients who booked for transport services on a particular date.

- **Inpatients Report** – this report is used by Consultants to view the patients' appointments scheduled on a particular date. This report is also used at the MDH reception area to search for a patient who has been admitted to hospital, whenever a relative or a friend asks for directions at the reception desk.

- **HL7 Audit** – this report is mainly used by the CPAS team to audit part of the HL7 messages sent from 00:00am onwards on a particular day, and would include amongst others the date, time, event ID, event track (whether a patient was registered/admitted/transferred/discharged from CPAS and by whom), etc.

Whilst reviewing the reporting functionality of this application, the NAO observed that a few other reports, such as the *'Patients Generic report'* and the *'Analysis report'* are still under development and will be introduced at a later stage. The NAO was informed that whilst most of the statistical reports from CPAS are handled by the Central Processing unit within MDH, end users could issue statistical reports from CPAS on the number of clinical appointments held over a period of time. The latter report highlights those patients who showed up for an appointment and were registered on CPAS, patients who did not show up for an appointment, patients who had cancelled an appointment and those patients who walked-in at the clinic or ward without an appointment as they were referred to by their Consultant/Doctor. The NAO was informed that if a patient did not show up for an appointment, the CPAS application has been configured to automatically flag the status field and mark the patient that he/she did not turn up for the appointment, after the lapse of 24 hours when the appointment was due. The NAO observed that when the end user exports such a report to Microsoft Excel, and filters the report according to the status field criteria and Consultant, the end user has to add them up manually since the system does not automatically add the total number of patients according to the status field criteria and Consultant. The NAO recommends that MDH should look into this and whether such a report can be modified to automatically add the total number of patients according to the status field criteria and Consultant.

Apart from the reporting functionality, the CPAS application has a *'Tracking Module'* whereby users can easily trace the whereabouts of every patient's personal file by scanning the file through a barcode reader. This *'Tracking Module'* is mainly used at MDH, whereby the barcode number from the user's MDH Identification tag is linked with the CPAS user account. Thus, through this *'Tracking Module'*, a user can easily trace the location of a patient's personal file, the date when the file was moved from one location to another and who requested the file. However, whenever a user requests a patient's personal file, the request is made with the Medical Records department from the KURA web application. These requests, which are considered as urgent, are normally related to patients who walked in for an appointment after being referred to by their Consultant/Doctor or if the patient's file was not brought up at the ward or clinic when they showed up for an appointment. In turn, the Medical Records department would process the request, trace the file and update the file location (where the file will be sent) before the request is closed from the KURA web application. The NAO was informed that it is envisaged that by the end of 2016, such requests would be registered directly from CPAS rather than using a third party application, thus eliminating the dependency on the KURA web application.

Finally, the CPAS application offers the functionality whereby Nurses who are assigned at the Medical or Surgical wards or at the Central Sterile and Supplies department, could record their time-off-in-lieu. A report could then be generated from CPAS indicating all the Nurses who recorded their time-off-in-lieu according to their location and the number of hours recorded. Such a report is normally endorsed by the Nursing officer and submitted to the Payroll section within MDH, through the Government e-mail. In turn, the number of hours submitted as time-off-in-lieu is recorded by the Payroll section in Dakar to ensure that they could keep track whenever a Nurse avails of a number of hours as time-off-in-lieu on a particular month.

3.4 Central Theatre Management System

The Central Theatre Management System (CTMS) application was developed by a local third party supplier, with the aim of automating the process by which Consultant surgeons or Physicians manage their patient waiting lists. It also facilitates the ability of the MDH administration to keep track of the number of patients on the waiting list and their current status. The CTMS application is mainly used at the Centralised Theatre System office (CTSO), the Clinical Performance unit, the Data Management unit and the Operating Theatres within MDH.

The CTMS application runs on a Microsoft SQL database and is currently hosted at MITA's SHE. As part of the hosting services contract, MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is backed up regularly. In this regard, the NAO was informed that the system is backed up through the *'grandfather-father-son'* backup rotation, whereby a full monthly backup to tape (*'grandfather'*) is scheduled on the first Friday of the month whilst a full weekly backup to tape (*'father'*) is scheduled on the remaining Fridays of the month. On the other hand, a full backup to disk is scheduled from Monday to Thursday. Thus, the *'grandfather'* set consists of 12 backup tapes, whilst the *'father'* set consists of four backup tapes. In total, 16 backup tapes are used and stored offsite by MITA.

At the time of the IT audit, the CTMS application was being maintained by one ICT Application officer within the IM&T unit, who provided first-line technical support to the end users within MDH when required, and liaised between the local third party supplier and MITA whenever any enhancements, software upgrades or technical assistance were required.

Whilst reviewing the CTMS application, in terms of user account management, the NAO was informed that whenever a new user needs to gain access to the CTMS application, an e-mail request is normally sent by the CTSO to the ICT Application officer. In turn, the ICT Application officer would create a new user account and grant access rights as stated in the e-mail request. In this regard, a user account can be provided access rights in line with any of the following user types:

- ***Super user*** – can create new users or edit details of existing users, edit lookup tables, upload appointment letters according to the speciality area, generate reports, access audit trails and view error lists.

- ***Aggregate/Statistical Report user*** – can only execute a limited number of reports.

- ***Clinical Chair + Consultant*** – a Clinical Chair has the same access rights as a Consultant. However, the Clinical Chair can access the waiting lists of all the Consultants according to their speciality.

- ***Consultant*** – can manage, view or generate a simple report on his/her waiting list and can also view activity log on his/her waiting list.

- ***Speciality Administrator*** – assigned to one Consultant from each specialty area. The Specialty administrator can access the waiting list of each of the assigned Consultants and has the same access rights as the Consultant role.

- ***Office Administrator*** – assigned to a number of Consultants that can spread across different specialty areas. The Office administrator can access the waiting list of each of the assigned Consultants and can avail of the same access rights as the Consultant role.

- ***Medical Administrator*** – have access to all the Consultants' waiting lists in all the specialty areas. The Medical administrator has the same access rights on the waiting lists as the Consultant role.

In the meantime, the NAO observed that the CTMS application does not offer any password security controls, in terms of password complexity, password expiry, and password history or block the user account after a number of unsuccessful login attempts. In this regard, the NAO is of the opinion that the ICT Application officer should liaise with the local third party supplier and enhance this application in terms of password security controls.

In the event that a user has forgotten his/her password, the user must send his/her request to the ICT Application officer through the Government e-mail. In turn, when a new password is generated, the ICT Application officer would send the new password by e-mail to the user's mailbox. Whenever a user retires or no longer requires access to the system, the NAO was informed that the user account is disabled only if the ICT Application officer is informed by the CTSO through the Government e-mail.

The same procedure applies for users who are on prolonged leave, career break or maternity leave. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed accordingly, and the respective user accounts are disabled.

The NAO noted that the CTMS has an audit trail in place to record amongst others: successful or failed login attempts according to the date and time, who created, modified or deleted data on CTMS, who retrieved information and accessed the Consultant's data etc. These audit logs can be retrieved from the back-end and can be exported in *'.pdf'* format. The audit data exported in *'.pdf'* format reflects the filtering criteria applied by the end user.

During the course of the IT audit, the NAO interviewed and observed key users within MDH on the use of the CTMS application. In this regard, the NAO was informed that Consultant surgeons or Physicians, who are granted access to the CTMS application, must ensure that all the elective and scheduled procedures are listed on the CTMS register, as soon as the operating procedure is identified, or within a week from when it is identified.

This function of inputting patient's data into CTMS may be delegated to any other member of staff, yet, the ultimate responsibility for the validity of such information rests with the Consultant surgeon or Physician who is performing the elective or scheduled procedure/intervention.

Similarly, when an elective or scheduled procedure/intervention is completed, the Consultant surgeon or Physician is responsible for closing the case him/herself or delegate another member of staff to close the case. As highlighted above, if the task is delegated to a member of staff, the Consultant surgeon or Physician is responsible for closing the case, once an elective or schedule procedure/intervention is completed.

The NAO was informed that there are occasions when a patient is contacted to undergo surgery, the patient is unable to have the surgery on the proposed date and thus a mutually acceptable date for the surgical intervention/procedure is scheduled accordingly. However, if the patient refuses to accept a date in the near future, the Consultant surgeon or Physician would inform the patient that such refusal might lead to the closure of the case from the CTMS application. Similarly, the case is closed if for some reason the patient fails to turn up more than once for the surgical intervention/procedure, rather than refusing to attend. In both instances, if the case is closed, the Consultant surgeon or Physician will inform the CTSO in writing that the case is closed. Meanwhile, the patient is also informed in writing by the CTSO, through a registered letter, that the case has been closed.

In the event that a case is erroneously inputted into the CTMS application, the Consultant surgeon or Physician must inform the CTSO to delete the case from CTMS. In addition, if the CTSO identifies a case, which may have been inputted by mistake, the CTSO contacts the Consultant surgeon or Physician in question and inform him/her accordingly. The latter would verify whether the case was erroneously inputted in the system and if the case needs to be removed, the CTSO is informed to remove the entry accordingly.

Likewise, if a case has been listed repetitively for the same procedure or intervention, the CTSO has the authority to remove duplicate entries following the necessary verifications with the respective Consultant surgeon or Physician. The NAO was informed that sometimes it is the case that a patient's case is listed in CTMS for the same procedure or intervention under two different Consultants. In this scenario, the CTSO would inform the patient and is given the option to select under which Consultant the case should be retained. If the patient is not in a position to select their preferred Consultant, the responsible Chair would take the decision on the patient's behalf.

Overall, the NAO observed that the CTMS application does not permit double entry bookings for the same procedure and thus the CTSO must close one of the cases in question within five working days from when the double booking entry is identified. In this regard, the CTSO continuously monitors all the entries that were recorded in the application and ensures that the respective users continuously update the CTMS application.

Furthermore, the NAO was informed that the Clinical chair monitors all the cases inputted in the system and ensures that all the necessary measures are taken into consideration to minimise the waiting time of patients who are on the waiting list and the progress of the waiting lists. In this regard, the Clinical chair may raise the issue with the Clinical director in the event that a Consultant surgeon or Physician's waiting list has reached the maximum waiting time and other Consultant surgeons or Physicians are available to conduct such procedures in an earlier time-frame. The Clinical chair would then make the necessary recommendations on how to address the situation, which might entail distributing the waiting list across the available resources and attempting to minimise the waiting time of patients who are on the waiting list. Subsequently, the CTSO is to be informed in writing to affect any changes on the CTMS application, especially if there is a shift in the procedure or intervention from one Consultant surgeon or Physician to another. However, all the above remains within the Management's prerogative to take such action when this is considered warranted.

Whilst reviewing the CTMS application, the NAO observed that the CTMS has a reporting functionality whereby users can extract useful information on patients' waiting lists.

- **Open Case Waiting List** – this report presents a summary of the open cases for a particular speciality area grouped by the intervention type and Consultant.

- **Open Cases Waiting List by Priority** – this report presents a summary of the open cases for a particular speciality area grouped by the intervention type, Consultant and priority.

- **Pending Cases** – this report presents a summary of the pending cases for a particular speciality area grouped by the intervention type and Consultant.

- **PWL Waiting Time** – this report shows the maximum and average waiting time for a particular speciality area grouped by the Consultant and intervention type.

- **Deleted Patient Cases** – this report presents a list of the deleted cases.

- **Closed Cases** – this report presents a summary of the closed cases for a particular speciality area grouped by the Consultant and intervention type. This report is only available to super users.

- **Case Movement** – this report presents a summary of the open cases for a particular speciality area and Consultant ordered by the date registered. The summary represents the order in which the cases are in the Consultant list. This kind of report is only available to super users.

- **MDH WL – CPU Data Extract** – this is a general report related to the MDH waiting list that can be exported to Microsoft Excel, so that the end user would be in a position to sort, filter and make the necessary changes required.

All the above reports, with the exception of the *'Deleted Patient Cases'* report have a set of filtering criteria, some of which are mandatory while the others are optional to the user, for a report is generated from the system. All the reports can then be exported and saved to Microsoft Excel or *'.pdf'* file format.

Finally, during the course of the IT audit, the NAO was provided with a detailed statistical report, showing all the interventions that were registered in the CTMS application from 1st January until 30th September 2015.

Clinical department	Number of operative/intervention episodes registered on the CTMS application
Anaesthesia (Pain Relief)	346
Cardiology	298
Dental	96
Medicine	1,044
Obstetrics & Gynaecology	480
Ophthalmology	1,539
Orthopaedics	7,064
Surgery (ENT)	1,291
Surgery (General Surgery)	3,541
Surgery (Urology)	1,223
Total number of interventions/procedures	**16,922**

Table 3 - The number of interventions/procedures registered on CTMS between January and September 2015

The report provided to the NAO took into consideration the following criteria:

- Newly appointed Consultant firms as well as consultants who are close to retirement may have fewer interventions registered on the CTMS than other Consultant firms.

- Different Consultant firms within the same broad speciality have diverse sub-specialities and thus only a few Consultant firms specifically carried out certain interventions.

In addition, a separate report was provided to the NAO showing the number of interventions, which were postponed or cancelled on the day between January to September 2015.

Reason why intervention was not carried out	Number of operative episodes
Postponed procedures	207
Patients did not turn up for procedure/intervention	404
Procedure/intervention not carried out due to Medical reasons	399
Other reasons (ex. Patient not starved, malfunction of machinery etc.)	84
Total number of operative episodes	**1,094**

Table 4 - Total number of interventions/operations not carried out on the day between January and September 2015

3.5 Cardiovascular Information System

The Cardiovascular Information System (CVIS) application is a comprehensive information management solution designed to provide users with convenient access to the complete and detailed records of all cardiac patients across the Cardiology department. Thus, all the clinical data, images and reports of the procedures performed at the Catheterisation laboratory (Cath lab), echoes done at the Cardiac laboratory (Cardiac lab), information related to the Cardiac Outpatient visits at the Medical Outpatients (MOP) 4, and the Pacemaker implantations and Pacemaker program checks, are stored on the CVIS application.

The NAO was informed that the patient's data is inputted in the CVIS application either manually through clinical forms, or automatically via a wide range of clinical modules that capture data during diagnostic, therapeutic and follow-up examinations, which are then stored in a single relational cardiovascular database. The latter is a Microsoft SQL database, which is hosted on a Microsoft Windows SQL Server residing at MITA's MDH Data Centre and used by the Cardiology department within MDH and GGH.

The CVIS application can also be used to generate clinical reports, patient letters and registry submissions, for all patients and procedures stored in the database. It also provides detailed operational information, such as patient scheduling, supply utilisation, as well as productivity and outcomes reporting.

At the time of the IT audit, the NAO was informed that a new service contract had just been concluded between MEH and the local third party supplier for the provision of hardware and software maintenance and support for the next five years. Furthermore, the NAO observed that this service contract stipulates that the existing hardware, including the server hosting the CVIS application and other hardware components will be replaced, whilst the CVIS application will be upgraded with the latest software release. However, the NAO observed that the service contract does not clearly state by when the existing hardware component will be replaced or when the CVIS application is updated to the latest software release.

In this regard, the NAO was informed that the new servers will be configured as passive/active and will be installed at MITA-01 Data Centre in St. Venera and MITA's MDH Data Centre respectively. Both servers will adopt the *'grandfather-father-son'* backup rotation, whereby an incremental backup to disk is scheduled on a daily basis, whilst a full backup to tape is scheduled weekly or monthly. The

backup media are loaded on to servers and kept off-site by MITA. Since both servers will be hosted at MITA, the backup process will be monitored by MITA. Thus, in the event that a backup fails, MITA will inform the CVIS System administrator who in turn will inform the local third party supplier to take remedial action. Moreover, if a file or system restore is required, the CVIS System administrator will liaise with MITA and the local third party supplier for the loading of the backup media on to server.

Whilst reviewing the CVIS application, the NAO observed that the system is maintained by a Principal Radiographer, in the role of a System administrator, and is assisted by the MITA Health Team and the local third party supplier when the need arises. The latter provides second and third line of support, according to the established SLAs, to provide amongst others:

- the supply and installation of emergency fixes, minor and major software releases of the CVIS application;

- the investigation and identification, where possible, of suspected faults associated with the CVIS application as reported by the CVIS System administrator;

- the supply of temporary software workarounds or software patches to overcome incidents reported by the CVIS System administrator; and

- technical assistance over the phone or on-site when applicable. Furthermore, the local third party supplier can also offer technical assistance remotely through a secure VPN connection.

The NAO is pleased to note that the local third party supplier, together with the CVIS System administrator and the MITA Health team, adhere to the Change Management procedures, whereby all the changes are carried out in a planned and authorised manner. This applies whenever there is a hardware fault, a software fix, or a new requirement is needed amongst others. The same applies if the hardware components need to be replaced or the software application is upgraded with the latest software release as highlighted above.

Furthermore, the NAO was informed that when a new software application release or update is installed, the local third party supplier would provide adequate training to the CVIS System administrator, who in turn provides training to users on a one-to-one basis. On the other hand, new users are provided on-the-job training by their respective work colleagues.

Whenever a new user wishes to gain access to the CVIS application, a *'Request for IT Service form'* is filled-in, signed by the relevant stakeholders and sent to MITA's Service Call Centre. MITA would then raise an incident request for the creation of folder on MDH's shared network drive and grant access rights to the respective user. The incident request is then escalated to the CVIS System administrator for the creation of a user account on the CVIS application. The NAO observed that whenever a new user account is created, the password is set with a minimum number of characters and the user must change the password upon first logon. Even though passwords are encrypted, the system does not offer any password security controls in terms of password complexity, password expiry, password history or block access after a number of failed login attempts. However, the NAO was informed that at

the time of the IT audit, a new service contract was being negotiated between MEH and the local third party supplier. In this regard, it is envisaged that with the new service contract, MDH will be looking into the possibility of enhancing the password security controls once all the hardware and software applications are upgraded.

In the event that a user has forgotten his/her password, the user can phone or send his/her request to the CVIS System administrator through the Government e-mail. A new password is generated and sent to the user's Government e-mail. The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is deleted only if the Charge nurse of the section informs the CVIS System administrator through the Government e-mail. A similar procedure is applied for users who are on prolonged leave, career break or maternity leave, whereby the user account is disabled until the user returns to work. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed, and the respective user accounts are disabled or deleted accordingly.

The NAO observed that whenever a new user account is created, the CVIS System administrator assigns access rights according to the user's job description. In this regard, the NAO noted that the CVIS application has four different user levels, namely:

- **Administrator** – has full access rights to print reports and images, finalise and unlock amended reports, merge patients and studies, add users and assign them to a clinical group, export and import to media, delete an ordered study, manage system wide work list, modify patient demographics, create and delete clinic diary schedulers, administer and create document templates, update stock, build and run queries etc.

- **Clerking user** – has rights to view only sectional reports, the scheduling facility for a section, and to print appointment letters.

- **Clinical user** – has rights to view only sectional reports, the scheduling facility for a section, print appointment letters and to finalise reports.

- **Physician user** – has rights to view report, print reports, and to finalise and unlock amended reports.

At the time of the IT audit, the NAO was informed that the CVIS application had around 100 user accounts from within the Cardiology department, but the CVIS application only allowed for 24 concurrent users. In the event that a CVIS user account is inactive for more than 30 minutes, the system automatically terminates the current session and free up a user licence. However, it is envisaged that with the new service contract, 40 additional concurrent user licences will be included once the CVIS application is upgraded with the latest software release.

Furthermore, the NAO was informed that the CVIS System administrator does not have visibility to any audit logs and thus cannot quantify whether the audit function is enabled and the type of logs that are

being recorded. In this regard, the NAO is of the opinion that the CVIS System administrator should clearly establish who has access to these audit logs, whether the audit log is enabled, what kind of logs are being recorded and how information can be retrieved if and when required.

Finally, the NAO was informed that the CVIS application is integrated with the CPAS application to retrieve patient demographics. Meanwhile, it is envisaged that with the implementation of the new CVIS software release and the replacement of all hardware components, the CVIS application is integrated with other MDH critical applications, such as the iCM application.

3.6 Dakar

The Dakar application was launched in 2003, when SLH was Malta's main general hospital before MDH became the public hospital in Malta in 2007. Throughout the years, the Dakar application was developed and customised to cater for the then SLH's requirements, and modified again when MDH became an acute general hospital in Malta as we know it today.

At the time of the IT audit, the Dakar application was hosted on a dedicated server, which was installed at MDH Data Centre. The NAO was informed that the Networks team within the IM&T unit were liaising with MITA on the possibility of migrating the Dakar server and application at MITA's SHE. However, due to the unexpected resignation of the Network's team personnel from MDH, the IM&T unit had to put aside the migration process until the ICT Application officers, who were entrusted with the responsibility of the Dakar server and application, become familiar with the system, before resuming with the migration process.

Whilst reviewing the Dakar server, the NAO observed that the Dakar application is backed up to disk on a daily, weekly and monthly basis. Upon successful completion, the backup application software installed on server has been configured to send e-mail notifications to the ICT Application officers' mailbox. The same procedure applies when a backup process fails. The NAO was informed that the backup file residing on server is backed up on to the primary NAS device, whilst the latter is then replicated on to a secondary NAS device. Both NAS devices are installed at MDH Data Centre. On a daily basis, the ICT Application officer logs on to the Dakar server and both NAS devices to ensure that the backup file exists in the respective folders. The backup files are then renamed according to MDH's naming convention to reflect the date when the backup was completed.

The NAO is pleased to note that to ensure the data integrity of the backup process, an ICT Application officer carries out a file restore every month, whereby the latest backup file is selected and then copied on to a stand-alone workstation installed at the MDH Payroll section. This stand-alone workstation is installed with Microsoft Windows XP operating system and runs various older versions of the Dakar software compatible with this operating system, with MDH payroll data dating back to 2005. In turn, an officer within the MDH Payroll section compiles a number of reports from the stand-alone workstation, and in doing so, indirectly verifies that data integrity has been maintained.

In the meantime, the ICT Application officers carry out a number of other functions in respect to the Dakar server and application. As part of their daily monitoring routines, the NAO observed that an ICT Application officer logs on to the Dakar server remotely and checks the *'Raid Manager'* application

and the *'Event Viewer'* logs for any system errors. If system errors are detected, the ICT Application officer will liaise with the local third party supplier and verify whether any intervention is required on site.

Furthermore, an ICT Application officer also monitors the Dakar's database growth by populating the current database size in a Microsoft Excel worksheet, and analyse the database growth through PivotCharts. On a weekly basis, an ICT Application officer extracts the information and forwards the report to key stakeholders within the MDH Finance Directorate and the IM&T unit.

In this regard, the NAO recommends that the ICT Application officers should liaise with the local third party supplier and check whether any server-monitoring tools can be installed on the Dakar server. Ideally, once these tools are installed, they are configured to send e-mail notifications to the ICT Application officers' mailbox, highlighting any alerts generated due to hardware errors or performance degradation, such as faulty Hard Disks, high CPU usage, overheating, or low disk space. Through these server-monitoring tools, the ICT Application officers would be proactive and take immediate action when an alert is prompted, if the server performance has degraded, or there is a hardware fault. Furthermore, considering the current manual monitoring process, these monitoring tools are more efficient and less time consuming.

Whilst reviewing the Dakar application, the NAO observed that the system is accessible through a login and a password, together with a dongle, which must be connected to every workstation on which the Dakar application is installed. All the Dakar user accounts are managed by the ICT Application officers, in terms of user account creation, modification or deletion, password management and user access rights. However, since every user account is linked to a user licence, the ICT Application officers should ensure that user licences are available before a new user account is created. Having said that, at the time of the IT audit, the NAO observed that the ICT Application officers could not quantify whether they have any free user licences or whether the current amount of 33 user licences is correct. Since these user licences come at a cost, the NAO recommends that MDH should clarify this issue with the local third party supplier and ideally keep a log listing each user licence and the PC or laptop inventory/ serial number on which the dongle is installed.

In the meantime, whenever a new user within the MDH Payroll section or the MDH Personnel section requires access to the Dakar application, the Head of Directorate sends an e-mail to the ICT Application officers, listing the name, surname, user login and the type of access that should be granted on the Dakar application. The NAO observed that a new user account is granted with the same access rights to an existing user account. In this regard, the ICT Application officer would search for a specific user account, as stated in the e-mail, click on the *'Copy Record'* icon, type in the new user login and rename the *'Full Name'* and *'Password'* fields accordingly. In doing so, the new account will inherit the same access rights as to an existing user account. However, even though the Dakar application offers a number of user levels, it might be the case that a user is granted more access rights than required. As a result, the NAO recommends that the current list of user accounts is extracted from the Dakar application and periodically verified with the relevant stakeholders so as to ascertain that every user has been granted access rights according to their role and responsibilities within their respective sections.

In addition, the NAO observed that whenever a new account is created and a password is set for the new user within the respective section, the password is not set as complex. Hence, the user is not forced to change password upon first logon, nor is the password set to expire over a stipulated number of days, even though the Dakar application offers the functionality to force password change or to set the number of days when the current password should expire. In this regard, the NAO was informed that user passwords have not been changed for a substantial amount of time. Thus, the NAO recommends that all the user accounts on Dakar should adhere to password management best practices, whereby the system will enforce the end user to change password upon first logon, the password should expire periodically, and must be set as complex with a minimum of eight characters in length, including a mix of letters, numbers and special characters. Alternatively, since the Dakar application is hosted on a dedicated server and not part of a Domain, once the Dakar server and application are migrated on to MITA's SHE, MDH should look into the possibility that the Dakar server is joined to the CORP Domain, and the current user accounts are integrated to the CORP Domain's Active Directory. Since the current workstations at MDH are already joined to the CORP Domain, the same user login and password could then be used on the Dakar application, thus inheriting the same password policies defined by MITA on the CORP Domain's Active Directory.

At the time of the IT audit, the NAO was informed that the audit trail functionality on the Dakar application was disabled as it was generating too many logs, which affected the performance of the system. Having an audit trail in place can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection and problem analysis. In this regard, MDH cannot currently identify who accessed the application, when and what data was inputted, modified or deleted in the Dakar application. Thus, the NAO recommends that key stakeholders within MDH together with the local third party supplier should review the current Dakar application and server specifications, and come up with a solution to re-enable the audit trail functionality without impacting the performance of the system.

Whilst reviewing the Dakar application, the NAO observed that this system is mainly used by the MDH Personnel section and the Medical Co-Ordination unit within the MDH Human Resources and Administration Directorate, and by the MDH Payroll section, which forms part of the MDH Finance Directorate.

Notwithstanding, MEH is responsible for the recruitment and engagement of new employees at MDH and in this regard, the MDH Personnel section is only informed of new recruits commencing employment at MDH when the relevant approvals and related documentation are received from MEH. Upon enrolment of the new employee, the relevant details are initially recorded on the MDH Dakar application, and from thereon, the MDH Human Resources and Administration Directorate is responsible for the processing of all employee services[5]. Subsequently, the employee data can be accessed by the MDH Payroll section to trigger the relevant procedures from their end.

[5] Employee services include amongst others study or voluntary leave; unpaid leave; family friendly measures; pensions, resignations or terminations; disciplinary action; as well as progressions, promotions, and extension/revision of contracts.

Nevertheless, MDH's payroll process forms part of, and is dependent on, the Government's centralised payroll process, whereby responsibility is shared between MDH, Gozo Central Salaries section and the PAHRO. In this regard, the MDH Dakar application is used by the MDH Payroll section to prepare only the initial part of the payroll for MDH's employees, which entails the processing of all adjustments of a *'variable'* nature[6]. On the other hand, all adjustments of a *'fixed'* nature[7], covering all Public Service employees, are processed by the Gozo Central Salaries section, using the Government's centralised payroll package. The latter is also used by PAHRO to conclude and execute the final part of Government's payroll, which includes the compiling and processing of all the data from both sources, to complete the payroll run and the issue of payslips.

Moreover, the Medical Co-Ordination unit depends solely on the MDH Dakar application to issue reliable *'Doctors Daily Duty Rosters'*, which are uploaded on the KURA portal.

The MDH Dakar application caters primarily for approximately 4,400 employees at MDH, as well as around 40 corporate FMS employees. The NAO was informed that around 1,700 roster variations are registered on the system, of which approximately 800 are currently active. Unique codes are used to identify each roster in the system, and each employee is flagged with the relevant code. The latter is used to identify employees' working days/hours, and to calculate the relevant allowances. In line with Government's payroll process, payments are effected every 28 days, which result in 13 payments throughout the year. Some of the allowances are similarly paid on a four-week basis, whilst others are paid at specific pre-determined intervals, staggered throughout the year. In addition, overtime is usually paid one month in arrears. The NAO was verbally informed that the total remuneration cost per annum amounts to around €140,000,000.

The MDH Dakar application is highly dependent on information received from various sections within MDH, as well as other external entities, some of which do not fall under the responsibility of MDH. Subsequently, the process relies on the accuracy of the data submitted, and is susceptible to instances where the information may be incorrect, incomplete, late, or might not even be provided.

The majority of notifications that need to be processed are official documents[8], printed lists, or instructions received through various e-mails. These are scrutinised by the applicable officer, to initially assess how the employee is affected, and then to process the related adjustments accordingly. In this regard, the MDH Dakar system relies heavily on human input and processing, which may be subject to a degree of human error.

During the course of the IT audit, the NAO interviewed and observed key users on the use of the system, and noted a number of findings, which are highlighted in this audit report, in both the business process and the Dakar application itself.

[6] Adjustments of a *'variable'* nature include variable deductions, variable allowances, and overtime.

[7] Adjustments of a *'fixed'* nature include basic pay, changes to basic pay, and fixed allowances or deductions.

[8] Official documentation in paper format includes official/formal letters of appointment, progression, etc., contracts, rosters, attendance sheets, and sick leave certificates amongst others.

The NAO was informed that the MDH Dakar application is a stand-alone system, and is not linked with the Government's centralised payroll package. Whilst Government also uses a Dakar application, however this was developed and customised separately at a later stage. Nonetheless, since MDH's payroll process is interlinked with the Government's payroll process, data has to be transferred physically, and on a regular basis, between MDH, Gozo Central Salaries section and PAHRO.

However, in spite of relying on the MDH Dakar application, the NAO observed that the MDH Payroll section also relies heavily on Microsoft Excel worksheets. In this regard, all *'variable'* adjustments for that particular periodic cycle inputted in the MDH Dakar application, are initially processed and captured in the *'Form 7'* report. Whilst these transactions are vetted, all the data in the *'Form 7'* report is also extracted and exported to Microsoft Excel. Any additional adjustments required from this point onwards are calculated manually, and inputted directly on the file exported in Microsoft Excel, rather than on MDH Dakar. This Microsoft Excel worksheet is the only source that is passed on to PAHRO to be uploaded, merged and processed in the Government's centralised payroll system[9]. Subsequently, when the final paylist has been issued, PAHRO sends an updated Microsoft Excel worksheet, with the final adjustments and the latest payroll data to MDH Payroll section, to be uploaded on to MDH Dakar application, to ensure that both systems are synchronised together.

In the meantime, at the time of the IT audit, the NAO was informed that all the relevant details and the wages of around 85 MDH part time employees were completely excluded from the MDH Dakar application. In this regard, all pertinent details were maintained on a *'White Card'* paper-based document, whilst the wages were calculated in Microsoft Excel worksheet. In spite of this, the NAO was informed that MDH was in the process of migrating all the above to the MDH Dakar application, and a parallel run was about to be executed. In this regard, the NAO recommends that this migration process should be carried out as early as possible, to ensure that all the relevant details and wages of the MDH part time employees are transferred on to the MDH Dakar application.

Whilst reviewing the process involved in preparing the *'variable'* adjustments, the NAO observed that due to the lack of any electronic attendance recording system at MDH, the attendance is recorded manually in around 700 different timesheets. The latter are printed in batches from the Dakar application on a weekly basis, as this may impact the performance of the Dakar application if all the timesheets are printed at one go. All the attendances recorded are examined for any changes in hours worked (such as change of duties or overtime) or absences (such as vacation, sick, absenteeism without any justification), thus necessitating an adjustment in the employee's roster or pay. Whilst any roster changes are then recorded in Dakar, if a payroll adjustment is required, this is either calculated automatically by Dakar, after selecting the appropriate code, or manually worked out by the officer. In the latter case, only the final calculation result and the relevant code are inputted in Dakar for further processing.

With regard to overtime, this is recorded and approved on separate overtime sheets. The latter are collected and vetted to ensure that overtime is endorsed by the respective officer-in-charge in the respective ward or section. These are then cross-checked with the employee's roster and vacation

[9] After this stage, the provisional paylist is issued by PAHRO and sent to MDH. Any other final adjustments that may be required at this point are reported to the Gozo Central Salaries section in the form of instructions for processing from their end. This is done as per procedures, directions and deadlines set by PAHRO.

leave, to establish the number of overtime hours. Since the Dakar application distinguishes between *'normal'* overtime and *'other'* overtime[10] in separate fields, the NAO noted that in the case of *'normal'* overtime, the user inputs the number of overtime hours and selects the applicable code/s in Dakar, which would then automatically calculate the overtime amount due. On the other hand, the user also has to manually work out the applicable overtime rate, and then apply this rate to calculate the actual amount of overtime due, when working out the *'other'* overtime. In this case, only this monetary amount is finally inputted in Dakar for further processing. As a result, whilst the *'normal'* overtime rate cannot be manipulated, the *'other'* overtime rate and the final monetary amount due are completely dependent on the officer's input, and thus the workings carried out separately from Dakar are prone to human error.

In addition, the NAO noted that the *'normal'* overtime entitlement to employees working on reduced hours, is currently being calculated manually and the amount due is inputted in the *'other'* overtime field. In this regard, even though the user utilises a specific code to indicate an employee working on reduced hours, the Dakar application is unable to process this correctly.

Meanwhile, during the course of the IT audit, the NAO examined a sample of *'normal'* overtime payments processed through the MDH Dakar application. The test aimed to verify and assess the validity of basic inbuilt controls relating to payroll processing. Subsequently, a number of erroneous *'normal'* overtime payments were identified, in which an incorrect (higher) overtime rate was applied, resulting in an overpayment being made. The system erroneously applied the standard *'normal'* overtime rate (x1.5), regardless from the fact that this had exceeded the preset maximum overtime capping, which was supposed to override the standard rate. During the sampled pay period, Pay 8 2015, this particular overpayment affected 11 individuals in one particular grade, and amounted to €443.75. This incident was also confirmed by key officers at the MDH Payroll section. Upon enquiry, MDH management claimed that the supplier had been contacted and the issued had been fixed.

The NAO also noted that the MDH Dakar application cannot process pro-rata calculations, affecting any type of *'variable'* allowance or deduction. In this regard, the critical system functions are fragmented and whilst employee pay data, relevant codes, rosters, attendances and absences are inputted and updated in the system, the application is unable to automatically work out any pro-rata amounts due, to reflect the effective date or time. The NAO was informed that pro-rata adjustments may be effected in the event of:

- engagement of new employees in between pay periods;
- receipt of any back-dated appointments, promotions or progressions;
- availing of a number of hours of vacation leave on a Sunday (affecting deductions of Sunday allowance);

[10] The other overtime field is used for payment of Sunday overtime, including backdated overtime for which approval documents were received late, overtime performed in a higher grade, topping up overtime difference following a backdated appointment/progression, overtime performe by an off-duty employee working between 1 and 4 hours on a Sunday, as well as overtime performed at other Health entities. This field is currently also used for payment of overtime work by employees on a reduced hours basis.

- changing to a different roster in between pay periods (affecting mostly public holiday allowance, nursing premium allowance, etc.);

- switching between full-time, part-time or reduced hours in between pay periods;

- resignations, retirements or terminations of employees in between pay periods; and

- payment of Government bonus, income supplement, and all regular allowances (such as specialisation allowance, paramedic allowance, etc.) to employees on reduced hours and part-timers.

Consequently, these pro-rata adjustments have to be calculated manually by the payroll officers, before inputting the amount due (allowance or deduction), and applying the relevant code/s, in Dakar. The NAO was also informed that some of these calculations are maintained by the payroll officer in Microsoft Excel worksheets.

Following the issues highlighted above, the NAO is concerned on the high dependency on manual input on the MDH Dakar application, making it prone to human error. To mitigate these risks, the NAO recommends that MDH's management reviews its payroll business process holistically, and assess the possibility of enhancing the current system. The aim is to automate the process as much as possible, as well as to minimise the dependency on the end users. Thus, the system should be capable of taking into consideration the knowledge of the MDH payroll conditions and procedures, which would entail having a built-in mechanism that is able to retrieve the available employee data, factor in applicable changes inputted in relation to rosters, attendances and absences, and link these with the system's internal calendar. The system would then be able to process attendance data automatically and perform the relevant adjustments required to the employee's pay. As a result, all the system functions are consolidated and the application is exploited such that the payroll adjustments are calculated automatically.

As highlighted earlier on, the Dakar application uses different codes to distinguish between each different type of absences (absenteeism, sick, vacation, marriage, maternity, parental, bereavement leaves, etc.). However, these codes are not available and visible for selection through a drop down menu in the respective field where they are used. In this regard, the NAO observed that the desired code has to be keyed in by the user, which are mostly learnt through the users' experience.

The NAO noted that in the *'Analysis*' menu, unless the leading zeros are inputted in the employee ID number field, an error message is displayed, as the application does not locate and retrieve the specific employee's details. As a result, the leading zeros have to be keyed in by the user, rather than completed automatically by the system.

When inputting an amount intended for a *'negative'* payroll adjustment (a deduction) in Dakar, along with the applicable code for deduction, the system does not process the amount as a deduction by default. As a result, during system testing, it was revealed that the amount will be processed as *'positive'* (an allowance) unless the user remembers to key in the negative sign ('–') in front of this amount.

Whilst this issue affects primarily adjustments of a monetary nature (allowances and deductions), the above also applies to adjustments made to time-off-in-lieu.

Additionally, when an unrealistic and substantially material amount, such as a four-digit figure or more, has been inputted as a payroll adjustment (an allowance or deduction), the Dakar application does not prompt or warn the user to ascertain that this is correct. Such an error can easily result through an oversight at the inputting stage by the user, such as forgetting or misplacing the decimal symbol ('.'), or pressing the same number key twice or more.

Furthermore, when a payroll adjustment or amendment to a roster has been manually inputted in the system, the Dakar application does not prompt the user to update, save and lock the data, to ensure that these are not modified by other users, and that the changes applied are taken into consideration and correctly processed by the system. In fact, the NAO was informed that some of the changes inputted may be *'lost'* rather than processed during the payroll run, resulting in erroneous payments (mostly affecting allowances), unless the user remembers to tick ('✓') the *'manual change'* box, which by default is blank, and press the *'lock/update all'* button, once the changes have been inputted. As a result, these procedures are very critical and failure or omission might also impact another user working on the same case, as the latest data, inclusive of any adjustments, would not be available.

In light of the above, the NAO is concerned on the level of reliance on the end users and the risk of human error. In this regard, the NAO recommends that MDH's management addresses the issues highlighted above to minimise the dependency on the end users, by ensuring that the necessary modifications are implemented on the MDH Dakar application.

The NAO was also informed that a number of functions are not being properly or entirely addressed by the MDH Dakar Application:

- After a specific report is issued from the system, all employees eligible to the Meal allowance are manually identified one by one, and subsequently each entitlement has to be calculated individually by the MDH Payroll officers, rather than being processed automatically by the MDH Dakar application.

- The MDH Dakar application does not offer an automatic alert mechanism highlighting employees who have availed off all, or are close to utilising most of their vacation leave or sick leave entitlements. Furthermore, a report, which lists all vacation leave or sick leave availed off by an employee during a particular period, and another report that identifies employees on long-term sick leave, are not available. As a result, in order to review all the vacation leave or sick leave utilised by an employee, the end user has to manually open each employee's *'Absences Calendar'* in the system, and visually check and count each vacation leave or sick leave instance, one by one.

- Moreover, the NAO was notified that the vacation leave pertaining to a number of foreign Medical officers, engaged on contract basis renewable every six months, is not accurately recorded in the MDH Dakar application. This stems from the fact that their date of employment, which reflects the start of the year for these employees, does not equate to the start of the

standard financial year as considered by the system (every 1st January), resulting in incorrect vacation leave balances. Consequently, each of these employee's (pro-rata) vacation leave entitlement and running balances have to be manually calculated by the officers within the Medical Co-Ordination unit.

- The starting and ending times of rosters pertaining to Doctors, may vary and may not be accurately recorded on the Dakar application. Consequently, this may impact the vacation leave hours availed and the remaining balances, unless the end users at the Medical Co-Ordination unit modify the vacation leave manually in the system.

- Following a change in policy, at the time of the IT audit, MDH employees can avail themselves of study leave in hours. However, the MDH Dakar application only records study leave in days, and as a result, the MDH Personnel section maintains a detailed list of study leave availed off in hours in Microsoft Excel worksheets.

- In addition, when recording a period of study leave at a stretch, this has to be marked on the employee's roster, on a day-by-day basis. Apart from relying on manual input, this process is rather laborious for users at the MDH Personnel section, when compared to maternity leave, where the whole leave period can be marked in one batch.

- The NAO observed that the system does not offer the functionality to automatically calculate the actual amount in hours, availed or added, as time-off-in-lieu. As a result, this has to be calculated manually and the result is inputted in the system for further processing.

- Moreover, time-off-in-lieu is not registered and shown on the MDH Dakar calendar, and as a result the user cannot view the relevant data at a glance. Furthermore, the '*Statistics*' menu does not provide enough information when accessing time-off-in-lieu. In this regard, the user can only view a list of dates, but cannot quantify the number of hours added or availed as time-off-in-lieu on each particular day. The NAO also observed that when generating a specific report concerning any MDH employee, whilst this report provides details regarding vacation leave and overtime, amongst others, this does not provide any information relating to time-off-in-lieu or full pay sick.

- Whilst the MDH Dakar application maintains records of MDH employee's time-off-in-lieu, the NAO was informed that the time-off-in-lieu of Nurses posted in wards and employees of the Central Sterile and Supplies department is not comprehensively maintained.

Similarly, the MDH's management should also take note of the above-mentioned issues and look into the possibility of automating the business process as much as possible, facilitating the use of the system, and enhancing the reporting mechanisms.

Moreover, it transpired that issues may arise concerning foreign employees, in cases when these are initially registered[11] on the MDH Dakar application with a tax number, instead of an official ID number, until the latter is obtained from the relevant authorities. When the ID number is eventually provided, the end users are unable to modify the original tax number and replace it with the new ID number, since this is unique field. Consequently, users either continue updating the existing profile, without recording the ID number, or else create a new record based on the ID number. However, since new records are not merged with the initial profile, any existing data is forfeited, resulting in incomplete employee history, redundant records and unreliable data. In this regard, the NAO recommends that, on a regular basis, MDH carries out a high level exercise to identify and merge such records, to ensure that data integrity and reliability is maintained.

During the course of the IT audit, the NAO also observed that the MDH payroll section receive a considerable amount of queries, which are either received by e-mail, or raised personally by the employees themselves[12]. These queries are often related to the employee's salary, and any claims of erroneous payments. In this scenario, every query is examined by the respective officer, providing the relevant feedback, and in certain situations a detailed breakdown is provided to the MDH employee. Additionally, if it results that payment was erroneous, in spite of the officers being authorised to create a corrective payroll adjustment in the MDH Dakar application, no higher level review and approval are being sought prior to rectifying the error and settling the issue with the employee. In addition, these payroll adjustments are not backed up by any workings or explanations, and there is the possibility that separate cases are tackled differently. There is also the risk of collusion and the likely probability that an overpayment remains unnoticed and unreported, possibly indefinitely, unless the employee steps forward.

In this regard, the NAO was informed that a manual document (*'Payroll Adjustment Form'*) has been introduced, to log case details concerning such adjustments, which must be endorsed by the respective employee. However, apart from this manual document, the NAO recommends that the system's audit trail is re-enabled without any further delays, to detect, when and who may have inputted, modified or deleted data from the MDH Dakar application.

In the meantime, apart from the use of the MDH Dakar application, the end users within the MDH Payroll section and the MDH Personnel section make widespread use of Microsoft Excel. In this regard, the NAO noted that Microsoft Excel worksheets are used amongst others to:

- keep track of hours claimed by Doctors working on reduced hours and calculate their respective allowances;

- log the hours claimed by all Doctors at the Accident and Emergency department and calculate their Extra Duty allowance and overtime due;

- log Doctor's absenteeism;

[11] Registration of new employees is essential to issue salary payments, grant access to MDH security doors, and claim free meal entitlement if applicable, amongst others.

[12] During the week, the MDH Payroll section is open for MDH employees during specific hours of the day. A substantial number of MDH employees were observed during the audit testing, personally visiting the office to enquire about their salary.

- log sick leave certificates presented which were long due;

- keep a record of employee applications received and processed, for study leave, sports leave, etc. and trace whether such applications were approved accordingly; and

- alert the end user whether any employee contract is about to expire to kick off the process of renewal or extension and retrieve the physical personal file in advance.

Furthermore, the NAO also observed that other than Microsoft Excel worksheets, the MDH Payroll section and the MDH Human Resources and Administration Directorate, also utilise a number of physical documents, such as the *'Arrival Report form'*, *'Leave Booklet'*, and *'Employee's Sick Leave Card'* amongst others. Whilst the NAO acknowledges the use of Microsoft Excel and a number of physical documents, the NAO recommends that the MDH's management reviews the above instances, and assesses the possibility whether any additional enhancements to the MDH Dakar application are required, or further user training is necessary, if such functionality already exists in the system.

Overall, the NAO noted that the main Dakar processes are dependent on a selected number of core personnel who have accumulated a high level of knowledge and experience in their respective areas. This poses the risk that in the event of a sudden absence/loss of these individuals, the entire process may be disrupted, and invaluable knowledge is lost. In this respect, the NAO recommends that these key individuals should compile a detailed procedural manual and possibly, a number of other users are selected and involved in critical processes.

Finally, from the overall feedback provided, it was gathered that whilst the local third party supplier provides specific training when a new module or enhancement is implemented, most of the users are only provided on-the-job training by their respective colleagues. However, MDH's management and the end users expressed their interest in being offered advanced training on the MDH Dakar application. Whilst the NAO encourages the provision of professional training for all the end users, it is recommended that such training should be ongoing.

3.7 Day Care Unit

The Day Care Unit (DCU) application, which was launched in 2013, was developed through a service contract, by a local third party developer. The system, which is hosted on a virtual server environment at MDH's Data Centre, has a Microsoft SQL back-end database and is accessible through a web browser by nurses and doctors at the Day Care unit within MDH. The aim of the DCU application is to create/modify/search for a patient appointment, to monitor patients after an operation and to keep a record of all medical/surgical interventions or endoscopy procedures held at the Day Care unit.

During the course of the IT audit, the NAO observed and interviewed how doctors and nurses within the Day Care unit make use of the DCU application. The NAO also reviewed how the ICT Application officers within the IM&T unit maintain the DCU application in their day-to-day operations.

The NAO was informed that since the MDH's Data Centre falls under the responsibility of the IM&T unit, the Networks team within the IM&T unit, were responsible for the daily monitoring and maintenance

of the virtual server environment. At the time of the audit, the NAO was informed that the Networks team together with MITA were in the process of migrating the virtual server environment, hosting a number of applications including the DCU application, on to MITA's SHE. However, the migration process came to a temporary halt, as the two officials within the Networks team resigned from their duties within MDH. As highlighted earlier in the report, as a remedial action, the Director Health Informatics appointed a team of ICT Application officers from within the IM&T unit to assist with the functions of the Networks team. In this regard, the NAO was informed that the team of ICT Application officers together with the Director Health Informatics were liaising with MITA and intend to proceed with the migration process, which should be completed by Q4 2015.

Furthermore, the NAO was informed that another ICT Application officer is responsible for the overall administration of the DCU application, in terms of account management, system health checks, and backups amongst others. The ICT Application officer also provides assistance to doctors and nurses within the Day Care unit when required, and liaise with the local third party developer whenever a new enhancement or a software upgrade needs to be implemented.

Whilst reviewing the DCU application, the NAO observed that this application has around 60 active user accounts, including two administrative user accounts, used by the ICT Application officer and the local third party developer respectively.

Whenever a new user wishes to gain access to the DCU application, the Nursing officer in charge of the Day Care unit sends a written request to the ICT Application officer through the Government e-mail. Additionally, the NAO observed that whenever a new user account is created, the password is created the same as the user login, however, since the system does not prompt the end user to change password upon first login, the end users are advised to change their password. Unfortunately, since the password is changed upon the user's discretion, most users prefer not to change their password and retain the same password as the user's login. Furthermore, the NAO observed that the DCU application does not offer any password security controls in terms of password complexity, password expiry, password history etc. In this regard, the NAO recommends the DCU application should adhere to password management best practices, whereby the system will enforce the end user to change password upon first logon. The password should expire over a stipulated number of days, and the password must be set as complex with a minimum of eight characters in length, including a mix of letters, numbers and special characters.

In the event that the password was changed and the user has forgotten his/her password, the user must send his/her request to the ICT Application officer through the Government e-mail. A new password is then generated and sent to the user's Government e-mail. The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is disabled only if the Nursing officer at the Day Care unit would inform the ICT Application officer through the Government e-mail. However, this is not always the norm, as the ICT Application officer is only informed through an e-mail upon the Nursing officer's discretion. The same procedure applies for users who are on prolonged leave, career break or maternity leave. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed accordingly, and the respective user accounts are disabled.

The NAO was informed that whenever new enhancements are required to the system, the Day Care unit's Nursing officer would raise the request with the ICT Application officer. If these enhancements can be added from the *'DCU admin console'*, (ex. adding a new Consultant to the existing drop-down list), an e-mail request sent to the ICT Application officer should suffice. However, if the new enhancements are required from the backend (ex. the creation of a new field or a new reporting functionality), these are implemented by the local third party developer. Nevertheless, if there is a cost behind such a change, these enhancements are implemented only after approval has been granted from the Director Health Informatics and MDH CEO respectively. In this scenario, the local third party developer would initially create these new enhancements on the DCU testing environment. These enhancements must be tested and approved by the originator (Day Care unit's Nursing officer) before these are implemented on the live environment. The NAO is pleased to note that the ICT Application officer keeps track of all the e-mail requests received from the Day Care unit's Nursing officer and all the changes implemented on the DCU application in a physical file, whilst the original e-mail is kept in an offline mailbox.

Whilst reviewing the DCU application to the Day Care unit, the NAO was informed that whenever a patient has an appointment and visits the Day Care unit, he/she must present their ID card together with their appointment letter at the reception desk. The officer at the Day Care unit reception desk will search for a patient by their ID card number and check the patient's demographics from CPAS application, before searching for the patient's details from the DCU application. Since the DCU application is not integrated with CPAS, the patient details are updated manually on both applications if changes are required, before admitting the patient. The same procedure applies when setting up an appointment, whereby the official at the Day Care unit reception desk will update the DCU application or the CPAS application if the patient's demographics do not match. In this regard, the NAO is of the opinion that the DCU application is integrated with the CPAS application to retrieve patient's demographics. As a result, the patient's demographics should only be updated centrally, from the CPAS application, thus avoiding any inconsistencies in patient's demographics and eliminating the duplication of work in maintaining such data on both CPAS and DCU application.

Whenever a patient is admitted at the Day Care unit and must remain at the ward for further observation after a medical intervention, the NAO was informed that as part of the hand-over process, the end users must update the *'Comments'* field in the DCU application. However, the NAO observed that if a patient is kept for a few days at the Day Care unit, maintaining such comments is a problem, since the '*Comments*' field is continuously being updated by the end users during the day (for hand-over purposes), by removing the previous comments and typing in new comments. Thus, since the comments could be easily modified or removed by different users within the Day Care unit, this may result in erroneous data being typed in and handed in during the hand-over process. At the time of the audit process, due to the fact that the comments are being overwritten, if an end user wishes to review the comments inputted the previous day, the end user has no other option but to contact the ICT Application officer to restore the data from the previous backups. In this regard, the NAO recommends that the DCU application should be modified so as to save all the comments typed into the system, according to the date and time and cannot be deleted or overwritten. As a result, all the comments can then be easily read on screen or printed by the end user.

The NAO was informed that if an end user has erroneously admitted a patient on the DCU application as *'Inpatient'*, the system does not offer the functionality to remove the data or update the admission status to *'Cancelled'* for instance. Thus, to cancel this admission, the end user has no other option but to mark the patient as discharged, which would not be the case. In doing so, erroneous information is being captured when issuing statistical reports on the number of patients admitted/discharged at the Day Care unit. Similarly, if an end user erroneously discharges a patient on the system, whilst the patient is still under observation at the Day Care unit, the end user cannot re-open the same instance. Thus, the end user has to open a new episode and admit the patient all over again in the DCU application.

When an end user admits or searches for a patient, the DCU application offers different menus/fields for patients who are treated for a surgical/medical intervention or are admitted for an endoscopy procedure at the Day Care unit. In this regard, the NAO was informed that the menus/fields assigned to cater for surgical interventions and endoscopy procedures are quite straightforward, whilst the menus/fields assigned to cater for medical interventions are more detailed and some of the end users are finding such menus/fields quite complicated. In this regard, the NAO observed that whilst certain users who were interviewed during the audit process are finding the DCU application useful in their day-to-day operations, a few others were not confident in using the system. In this regard, these end users are attributing this to the lack of user training that was provided in using the DCU application.

The NAO is of the opinion that the ICT Application officer together with the Day Care unit's Nursing officer should take into consideration the above issues and find a solution to ensure that the DCU application reflects the business process of the Day Care unit. Furthermore, the NAO recommends that more hands-on training or refresher courses be held from time-to-time to ensure that all the users are confident in using the DCU application.

3.8 Electronic Case Summary

The Electronic Case Summary (ECS) was developed in-house by an ICT Application officer within the IM&T unit. The ECS application is used by medical doctors to compile an official hospital case summary (discharge letter) in electronic format. At the time of the audit, apart from MDH, the ECS application is also used at the GGH, Karin Grech Rehabilitation Hospital and SAMOC, and once the system testing is completed, the ECS application would also be implemented at MCH.

During the course of the IT audit, the NAO observed and interviewed how the ECS application is being maintained by the ICT Application officer, and how the system is used by Medical doctors in different wards across MDH to compile a patient's case summary report.

The NAO was informed that the ECS application has a Microsoft SQL back-end database and a web application front-end and is hosted at MITA's virtual segregated environment. MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is backed up regularly. On the other hand, the ICT Application officer provides assistance and user training to Medical doctors when required. Furthermore, the ICT Application officer monitors the Microsoft SQL database, in terms of error logs, storage, and backups amongst others. The ICT Application officer also offers first line technical support, and assists the Medical doctors whenever

an electronic case summary needs to be re-opened for further amendments, or a new functionality is required and added to the system.

Whilst reviewing the ECS application, which is accessible from an Internet browser through a login and a password, the NAO noted that a case summary could be initiated by a Medical doctor and continued by another. To compile a new case summary, the Medical doctor must input the patient's details first. Since the ECS application is integrated with the CPAS application, when the patient's ID card number is inputted in the '*Hospital ID*' field, the patient's demographics will automatically be displayed on the screen. On the other hand, if the patient's details are not displayed, the Medical doctor must then input all the patient's details manually. In this regard, the NAO recommends that whenever this is the case, the Medical doctors should report this to the IM&T unit to ensure that all the patient's demographics are updated and kept centrally on CPAS.

The next step is to select the *'Admitting Consultant', 'Admitting Ward', 'Admission Method', 'Admission Source', 'Discharging Consultant', 'Discharging Ward'* and *'Discharge Destination'* from the adjacent drop down menus and input the relevant data in each field. Furthermore, both the *'Admitting Date'* and the *'Discharging Date'* can be inputted through the *'Show Calendar'*, whilst the '*Discharging Date*' could also be inputted by pressing the *'T'* button, which refers to today's date when the case summary is being compiled. The Medical doctor, who is compiling the case summary, must type in their '*Name*' and *'Surname', 'Designation', 'Qualifications'* and their *'Medical Registration Number'* in free text. Upon saving, a new window is displayed on screen showing a number of options under the *'Case Summary Menu'*, whereby the Medical doctor can draft the discharge letter. The latter will include all the clinical details, which are typed in free text by the Medical doctor, and six separate fields for entry of diagnosis.

While reviewing the process of inputting all the necessary information in their respective fields, the NAO observed that the ECS application is also integrated with the iCM application. From the *'Case Summary Menu'*, the Medical doctor can collect all the patient's investigations from iCM, by clicking on the respective button, and retrieve all the investigation results on screen from the date of admission of patient until the current date. The Medical doctor can then select any of the results and import them from iCM on to the ECS application.

The case summary may also include any surgical procedures that the patient underwent, any complications that might have occurred during the patient's stay, the medical treatment to be given to the patient on discharge and any known allergies and/or other allergies that were noted during the patient's episode. From the *'Case Summary Menu'* the Medical doctor may also prescribe drugs, which can be of three types: urgent supply (three-day supply), free supply (two-three month supply) or the prescription for Private Use. The case summary may also include any pending results and any scheduled Laboratory or Radiology investigations. Furthermore, follow-up appointments may also be written in free text in the respective text box.

Once all the information has been compiled, the Medical doctor who closes the case will take the final ownership of the case summary. After closing a case, the ECS application has a 24-hour time window during which the Medical doctor or the discharging Consultant, who had closed the case, can

make further amendments to a particular case summary. In the event that a case summary needs to be amended after this period, the individual who had closed the case must send an e-mail to the ICT Application officer to unlock it. In this scenario, the NAO was informed that whenever a case summary is re-opened, the ECS application will automatically copy the case summary in *'.pdf'* format, to retain the original copy in the system (which is stored on the server), before the required changes can be made in the respective case summary.

From the ECS application, the Medical doctor can print a number of forms, such as the discharge letter, which must be handed to the patient before he/she leaves hospital, a prescription form that includes any drugs recommended to the patient by the Medical doctor, and a treatment guide form. The latter lists the drugs prescribed to the patient, the dosage and the frequency of use over a period of time. Such forms can only be printed once a case summary is closed. In the meantime, the hospital management sometimes requests ad-hoc reports, which are normally generated from the system, using Crystal reporting functionality.

At the time of the IT audit, the NAO observed that the ECS application had around 1,044 active user accounts including accounts used for testing purposes. Whenever a new user account is created, the system will prompt the end user to change the password upon first logon. The NAO was informed that all passwords are encrypted and that the ECS application has a password complexity rule in place, whereby the password must be set with a minimum of eight characters in length and must include a mix of letters and numbers. However, the NAO observed that passwords do not expire, old passwords can be re-used, and the system does not block access after a particular number of unsuccessful logon attempts. The NAO is of the opinion that the ECS application should adhere to password management best practices whereby the password history rule should at least be implemented, whilst passwords should be made to expire periodically.

In the event that a user has forgotten his/her password, the user either phones the ICT Application officer during office hours, or sends his/her request to the ICT Application officer through the Government e-mail. A new password is then generated and sent to the user's respective Government e-mail, which must then be changed upon first logon. The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is disabled. The same procedure applies for users who are on prolonged leave, career break or maternity leave. However, in every circumstance, user accounts are only disabled if the MDH Personnel Section informs the ICT Application officer through the Government e-mail. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed accordingly, and the respective user accounts are disabled.

The NAO observed that whenever a new user account is created on the ECS application, the ICT Application officer assigns access rights according to the user's role. In this regard, the NAO noted that the ECS application has four different user levels, namely:

- **View-Only access** – this user role is only granted to Nursing officers within the Renal unit and Urology department, for viewing purposes only.

- **Read-Write access** – this user role is granted to Medical doctors to compile and issue a case summary, or to search and view previous case summaries.

- **Hospital Activity users** – this user role is granted to specific users to view ECS episodes, for the clinical coding of patient diagnosis, according to the international statistical classification - ICD-10 codes.

- **Administrators** – this user role is solely used by the ICT Application officer and comprises of full access rights for the overall management of the ECS application.

The NAO is pleased to note that the ECS application has a number of audit trails in place, to record amongst others: successful or failed login attempts according to the date and time, from which PC or laptop the ECS application was accessed, who searched for a particular case summary, who created, modified or deleted data on a particular case summary etc. These audit logs can be retrieved from the back-end and can only be accessed by the ICT Application officer if and when required.

Furthermore, the NAO acknowledges that the ICT Application officer ensures that any changes made to the system are reflected on the *'ECS User Manual'* and the *'ECS Design Document'*. If new enhancements to the ECS application are required, a request is forwarded to the Director Health Informatics through the Government e-mail. The Director Health Informatics will discuss and address these requests with the ICT Application officer, and if these new enhancements are deemed fit, they are approved and implemented according to the software development lifecycle. The NAO was also informed that all the changes are recorded and adhere to the Change Management procedures.

Finally, with respect to user training, the NAO was informed that the Malta Foundation Programme[13] normally offers on-the-job training on the use of the ECS application during Foundation Year 1. The Malta Foundation Programme, which is a two-year training programme for newly graduated doctors, consists of structured training, hands-on training and assessments whilst working in a supervised hospital (MDH, GGH, SAMOC etc.) or primary-care environment. However, the ICT Application officer also provides assistance and user training to Medical doctors if and when required.

3.9 iSoft Clinical Manager

The iSoft Clinical Manager (iCM) application is an off-the-shelf application that was implemented in 2007, following the migration of SLH to MDH. iCM is a consolidated application that provides electronic patient demographic data, visit history, order entry, results viewing and patient documentation. Through the iCM application, users can send orders for laboratory tests and medical imaging, view the patient's results of laboratory tests and the reports on medical images.

The NAO was informed that the iCM application is a very critical software application that is used across MEH, including amongst others MDH, SAMOC, GGH, MCH, Karin Grech Rehabilitation Hospital, all Health Centres across the Maltese islands, the Health Head office, the Health Promotion unit etc. Furthermore, other entities or departments that do not fall under the remit of MEH, such as the Police

[13] http://fpmalta.com/

Headquarters, Corradino Correctional Facility, SVPR, Government Homes for the elderly etc., also have limited access to the iCM application.

At the time of the IT audit, the iCM application was running on a Microsoft SQL 2000 database and is hosted on different servers, which were installed at MITA-01 Data Centre in St. Venera and MITA's MDH Data Centre respectively. The iCM servers were configured with the *'grandfather-father-son'* backup rotation, whereby a differential backup to disk was scheduled on a daily basis, whilst a full system backup to tape was scheduled weekly or monthly.

As part of MITA's Hosting Services Contract, MITA is responsible for the hosting and monitoring of servers in terms of hardware and network infrastructure, the loading and storage of backup media and the monitoring of the backup process. In the event that a backup fails, MITA will inform the ICT Application officer and the Hospital IT Systems administrator who in turn will inform the MITA Health team. If a file or system restore is required, the officers will liaise with MITA for the loading of the backup media on to the server.

In the meantime, since the hardware components of the current servers are quite old and Microsoft no longer supports the current SQL 2000 database, it is envisaged that the iCM application is upgraded from the current version 1.4 to version 2.0 once sufficient funds are allocated for the whole project. This will entail the procurement of new servers, the upgrading of the current Microsoft Operating System, Office applications and SQL database, and the removal of unsupported software applications. Furthermore, the iCM application upgrade will include a number of enhancements over the current iCM version 1.4.

The iCM application is integrated with a number of critical applications that are in use within MDH. For instance, iCM is integrated with the CPAS application to retrieve patient demographics and patient visit details, whilst a user can also send orders from iCM and retrieve laboratory results through the LIS application.

During the course of the IT audit, the NAO was informed that the iCM application is monitored and maintained by an ICT Application officer and a Hospital IT Systems administrator within the IM&T unit at MDH. They provide first line technical support to all iCM users in terms of user account management, handling of printing services requests, creation of forms and monitoring the iCM application for any system or communication errors. The MITA Health team and the third party supplier assist the officers in providing second or third line technical support in respect of system maintenance, enhancements or software upgrades. In this regard, the NAO was informed that the third party supplier would liaise with the MITA Health team and access the iCM servers remotely through a secure VPN connection, if further technical assistance is required.

Whenever a new user wishes to gain access to the iCM application, a *'Request for IT Service form'* is filled-in, signed by the relevant stakeholders and sent to MITA's Service Call Centre. In turn, MITA will raise an incident request for the creation of a user account on iCM, and since the iCM servers are members of the CORP Domain, the user's CORP Domain account is added to the iCM user groups in Active Directory. The incident request is then escalated to the ICT Application officer and the Hospital IT Systems administrator for the creation of a user account on the iCM application. The NAO

observed that whenever a new user account is created, the password is set with a minimum number of characters but the system does not force the user to set complex passwords. However, the NAO observed that whilst previous passwords cannot be re-used, passwords do not expire even though the system offers the facility to set a password to expire on a specific date. Furthermore, the system does not block access after a number of failed login attempts.

In the event that the user has forgotten his/her password, the user must phone MITA's Service Call Centre, whereby an incident request is raised and escalated to the ICT Application officer and the Hospital IT Systems administrator. A new password is then generated and sent to the user's Government e-mail. The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is de-activated only if the ICT Application officer and the Hospital IT Systems administrator are informed through the Government e-mail. A similar procedure is applied for users who are on prolonged leave, career break or maternity leave, whereby the user account is disabled until the user returns to work. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed accordingly, and the respective user accounts are disabled or deleted accordingly.

Whilst reviewing the iCM application, the NAO was informed that the ICT Application officer and the Hospital IT Systems administrator maintain a detailed list of all user accounts in a Microsoft Excel worksheet, which is shared with the IT Trainer on the MDH network. In this regard, the NAO observed that new iCM user accounts are not forwarded to the user unless they attend to specific training and sign the *'User IT Training Record Sheet'*. Thus, whenever a new user attends to training on iCM, the IT Trainer will provide the user credentials to the user, and since the system does not prompt the user to change password upon first logon, the IT Trainer shows the user how the password is changed from iCM. Upon successful logon, the IT Trainer verifies whether the appropriate access rights to specific order sets were provided according to the user's speciality area, level, grade etc.

Apart from user training, users may also refer to some reference manuals or quick guide pamphlets, which were created internally by the IT Trainers, and can easily be downloaded from this unit's website. Furthermore, the iCM application offers an online *'Help'* functionality whereby the user can easily access the *'User Guide'* or search for a particular instance.

The NAO observed that the iCM application has an audit trail that records amongst others the date and time when a particular field was created or updated, the user's login, the name of the workstation, whether a document/form was signed, revised or cancelled, the reason why it was cancelled, who modified all these processes etc.

Furthermore, the NAO was informed that the ICT Application officer and the Hospital IT Systems administrator provide first line technical support on iCM's printing services and assists the IT Technical Support team within MDH whenever a new printing device is installed or replaced on the MDH network infrastructure. Through iCM's *'Report Manager'*, the officer can create print queues, modify existing print queues or view scheduled print jobs. In the event that a particular print job is stuck, the officer can clear/delete print jobs from the *'Report Manager'*, phones the user to check whether the problem can be solved over the phone or else call on site if the problem is within MDH premises. If the problem is

outside MDH, such as Health Centres, an incident request is raised with MITA's Service Call Centre and escalated to the respective Technical Support Contractor. At the time of the IT audit, the NAO observed that the ICT Application officer and the Hospital IT Systems administrator maintained a detailed list of around 157 printers in a Microsoft Excel worksheet. The latter includes details describing how these printers are configured in iCM, where they are installed and the contact number to reach the Nursing officer in charge of that particular section. The Microsoft Excel worksheet is continuously updated, and whenever an existing print queue is modified or a new print queue is created on iCM, an updated list is sent to the MITA Health team and the IT Technical Support team through the Government's e-mail.

As highlighted earlier, since the iCM application is integrated with a number of critical applications, on a daily basis the ICT Application officer and the Hospital IT Systems administrator check for any communication or system errors through a monitoring tool. In the event that errors are reported, the officers will liaise with the respective (CPAS, RIS, PACS, LIS) ICT Application officers to take the necessary action and resolve the errors.

Furthermore, as part of their daily routine checks, the ICT Application officer and the Hospital IT Systems administrator issue a report originating from CPAS on patients who were registered with a temporary ID number. The patients could be either newborns, who were provided with a temporary ID number from the Medical Records department until the newborn is registered with the Public Registry by the respective parents, or else individuals who were admitted to hospital in an emergency situation without valid identification. Based on these reports, when a patient is discharged and the episode is closed, the officer will search for the temporary ID number in iCM and change/merge the patient's records with a valid ID number accordingly. The scope of this report is to ensure that valid ID numbers are recorded in iCM, and in the event that a patient is re-admitted to hospital, the Doctors/Nurses could easily view the entire patient's medical history.

Finally, the NAO was informed that sometimes the ICT Application officer and the Hospital IT Systems administrator receive a request by e-mail for the creation of new forms in iCM. In this regard, the officers have access rights to create such forms on the iCM testing environment. Once the new form is created on the iCM testing environment, it is then tested by the officer and the originator, and upon approval, the form is then implemented on the iCM *'live'* environment. If training is required on the use of these forms, this is either provided on a one-to-one basis by the officer who created the form, or by the IT Trainer, if more than one individual requires training in a classroom environment.

3.10 ID Tag System

The ID Tag system was developed in-house in 2005, by an ICT Application officer within the IM&T unit. The system is solely used by two office Clerks at the Identification Cards office within MDH, to issue ID Tags for all MDH and SAMOC personnel and to other individuals who are not employed by MDH but are giving a service within MDH.

The NAO was informed that the ID Tag system, which has a Microsoft SQL back-end database and a Microsoft Access front-end, is hosted at MITA's virtual segregated environment. MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is backed up regularly. On the other hand, the ICT Application officer provides assistance and

user training to the office Clerks when required. Furthermore, the ICT Application officer monitors the Microsoft SQL database, in terms of error logs, storage, and backups amongst others, offers first line technical support, and assists the office Clerks whenever a new functionality is required and added to the system.

During the course of the IT audit, the NAO observed how the ID Tag system is being used at the Identification Cards office and the process involved in the issuing of ID Tags. The NAO noted that MDH personnel must fill in an *'Arrival report'* and a *'Roster form'*, which must be signed by his/her superior and a number of stakeholders within MDH. Whilst the *'Arrival report'* is handed in to the Personnel section within the MDH Human Resources and Administration directorate, the *'Roster form'* is handed in to the Payroll section within the MDH's Finance directorate. All the requests to issue ID Tags are processed through an e-mail, which must include the approval of the respective Head of Section.

Upon approval, the NAO observed that whenever MDH personnel call at the Identification Cards office, the employee details (ID Card number, Name and Surname, Designation, Section, Access level and Signature) are written down on the *'Card Log'* register file next to the ID Tag Card number. The same employee details are then inputted in a *'Card Log'* Microsoft Excel worksheet. In this regard, the NAO noted that certain fields, such as address and phone number are left blank due to the fact that such details are stored and can be retrieved from the Dakar application. In the case of non-MDH employees, a separate *'Card Log'* Microsoft Excel worksheet is kept to store such details.

Once all the details have been inputted in the respective worksheets, the Identification Cards office would then input the employee details again in the ID Tag System. The next step is to take a photo of the individual and then generate two barcode numbers. The latter are displayed on the ID Tag, whereby the first barcode number is scanned against a barcode reader by MDH personnel to track personal Medical History files when using the CPAS application. On the other hand, the second barcode number is used by MDH personnel to verify whether the individual is entitled to a free meal or not, when scanned to a barcode reader. This meal entitlement feature, which is applicable to MDH personnel only, is kept in a separate program and is linked to the Dakar application. The final step is to print the ID Tag using a thermal desktop printer that is attached to the PC where the ID Tag system is installed and hand the card to the individual, who in turn must sign on the *'Card Log'* register file.

To some extent, the same procedure is applied whenever an ID Tag is issued for non-MDH employees. However, non-MDH employees incur a one-time fee of €10 upon the issuance of an ID Tag, which is then reimbursed only upon the return of the ID Tag to the Identification Cards office. Furthermore, non-MDH employees are not entitled to a free meal nor have access to CPAS application to track personal Medical History files.

The NAO was informed that if the ID Tag is lost, a non-refundable fee of €7 is incurred upon the issuance of a new ID Tag, irrespective of whether the applicant is a MDH or non-MDH employee. Finally, all the ID Tags that are no longer in use and are returned to the Identification Cards office are destroyed and all the details are removed from the system.

Whilst reviewing the process involved in the issuing of an ID Tag, the NAO observed that both office Clerks within the Identification Cards office access the ID Tag system with a shared login and password

and that the system does not have any password security controls in place in terms of password history, expiry etc. While this goes against password management best practices, the NAO was informed that since the ID Tag system is only used to input personal details and print ID Tags, the MDH did not feel it was necessary to implement such an approach when only two users access this system. However, the NAO is of the opinion that since personal details are being stored in the system and only two office Clerks are accessing it, two separate user accounts are created and the password should at least expire over a stipulated number of days.

With reference to the audit logs, the system keeps an audit trail of all the ID Tags printed, the date and time and to whom they were handed. These logs are normally exported on to Microsoft Excel and used for billing purposes to distinguish between MDH/SAMOC and non-MDH employees.

Finally, the NAO is of the opinion that MDH should find a solution to avoid the manual repetitive work in inputting employee details in different areas. Ideally, MDH should stick to just the *'Card Log'* register file, as proof that the ID Tag has been issued and handed in to the respective applicant, whilst all the relevant details are kept centrally on the ID Tag system. Furthermore, the ID Tag system should clearly distinguish between MDH/SAMOC and non-MDH employees for billing purposes, and personal details should be kept for a reasonable pre-determined retention period, as per the provisions laid down in the Data Protection Act, and not removed once an ID Tag is returned to the Identification Cards office if it is no longer required. In this scenario, the ID Tag system should offer the functionality to input the date when the ID Tag was returned and include the reason behind it.

3.11 Laboratory Information System

The Laboratory Information System (LIS) application is an off-the-shelf system that helps scientists, technicians and management staff track samples and test several laboratory processes through a computerised system. Thus, it serves as a repository for laboratory test results and provides pathology reports that are electronically available to other hospital systems.

In this regard, the LIS application is integrated with a few other applications in use within MDH, such as the CPAS application to retrieve patient demographics, and the iCM application, whereby users can send electronic orders for investigation, and the results of all the order requests can then be easily viewed from iCM. Furthermore, the LIS application is also integrated with 43 different analysers, which receive requests and send results within the system. Once a test is authorised, either by Scientists or by the application, the results can then also be retrieved from the iCM application.

The LIS application was launched at the end of 2007 and it was first implemented at the Pathology department within MDH. The system was then extended to the Laboratory department at GGH and is also accessed remotely from the University of Malta, the Department of Health Information, the Accident and Emergency department and the Genitourinary (GU) clinic within MDH.

Notwithstanding, the NAO was informed that the LIS application is made up of four main laboratory disciplines, namely Blood Sciences, Blood Bank, Microbiology and Cellular Pathology and is mainly used at the Pathology department within MDH. The Pathology department investigates the causes of illnesses and how these progress, by carrying out scientific tests on tissue, blood and other samples

from patients. As a result, the department plays a crucial role in the diagnosis of diseases and by helping Doctors/Consultants choose the best type of treatment for patients and monitoring its effectiveness.

The NAO observed that the laboratory reception desk within the Pathology department operates 24/7 and receives most of the samples from within MDH through the pneumatic tube system, whilst samples from other centres arrive by courier. In most cases, samples arriving at the Pathology department will already have a barcode label, generated by iCM, attached to every sample and the corresponding request form. All the samples are checked for ID, sample suitability and proper authorisation, and are then grouped according to the section. The results of all the requests that are generated electronically from iCM can be viewed from the respective wards within MDH once they are marked as *'clinically approved'* from the LIS application. Furthermore, sample results can also be printed and sent to the respective wards within MDH through the pneumatic tube system.

At the time of the IT audit, the LIS application was running on six active/passive servers that include four Microsoft Windows Terminal servers and two Caché Database servers, all of which were hosted at MITA-01 Data Centre in St. Venera and MITA's MDH Data Centre. The LIS servers were configured with the *'grandfather-father-son'* backup rotation, whereby a differential backup to disk is scheduled on a daily basis, whilst a full system backup to tape is scheduled weekly or monthly.

As part of MITA's Hosting Services Contract, MITA is responsible for the hosting and monitoring of servers in terms of hardware and network infrastructure, the loading and storage of backup media and the monitoring of the backup process. Furthermore, every quarter, a test restore is carried out at random from the backup pool, to ensure that the data can be restored in the event that a file or system restore is required. In the event that a daily/weekly/monthly backup fails, MITA will inform the LIS System administrator to liaise with the MITA Health team to take remedial action if and when required.

During the course of the IT audit, the NAO interviewed key stakeholders and observed how the LIS application is being used at the Pathology department. In this regard, the NAO observed that two System administrators, who work on a four-day 12-hour shift, manage the LIS application. They provide assistance both within the Pathology department and other entities who were provided access to the LIS application. In this regard, the role of the LIS System administrator is to maintain user accounts in terms of the creation, modification or disabling of user accounts, handle password change requests, assign user levels, create reports and rules, maintain tables, handle printing requests, and monitor the system to ensure that no communication or system errors are being reported.

Since the LIS System administrators work on a four-day 12-hour shift, one System administrator can also access the LIS servers remotely after office hours, through a secure VPN connection, to assist users if and when required. In the meantime, the MITA Health team and the third party supplier assist the LIS System administrators in providing second or third line technical support, in terms of system maintenance, enhancements or software upgrades and both can access the LIS servers remotely through, a secure VPN connection, if further technical assistance is required.

Whenever a new user wishes to gain access to the LIS application, a *'Request for IT Service form'* is filled in and signed by the relevant stakeholders. These forms are handed to the IT Support Services team

within the IM&T unit to raise the necessary eRFS with MITA. In turn, MITA will raise an incident request for the creation of a user account on LIS, and since the LIS servers are members of the CORP Domain, the user's CORP Domain account is added to the LIS user groups in Active Directory. The incident request is then escalated to the LIS System administrator for the creation of a user account on the LIS application. The latter will create an account on LIS and grant access to particular disciplines according to the user's role within MDH or other entity/department. If a user requires access to view patient report across different disciplines, only the Chairman of the Pathology department can approve such a request.

Furthermore, the NAO was informed that for each sub-discipline a user is appointed to take the role of a *'super user'* to act as an expert in all LIS functionalities pertaining to that particular discipline. Furthermore, the *'super user*' liaises between the LIS System administrator and all the users within that particular discipline on any LIS related issues that might crop up, or on any new ideas/suggestions that have been brought up regarding possible improvements to the current system processes.

The NAO observed that whenever a new user account is created, the password is set with a minimum number of characters but the system does not force the user to set complex passwords. On the other hand, the NAO observed that previous passwords cannot be re-used, whilst passwords expire over a stipulated number of days and the system blocks access after a number of failed login attempts. Furthermore, the NAO was informed that if the password is not renewed within the stipulated period, the user account is automatically disabled by the LIS application.

In the event that a user has forgotten his/her password, the user is requested to phone MITA's Service Call Centre, whereby an incident request is raised and escalated to the LIS System administrators. However, there may be instances where the user phones or sends an e-mail to the LIS System administrator for assistance. A new password is then generated and given directly to the user over the phone, unless the user is physically present at the LIS System administrator's office. The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is disabled only if the LIS System administrators are informed through the Government e-mail. A similar procedure is applied for users who are on prolonged leave, career break or maternity leave, whereby the user account is disabled until the user returns to work. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed, and the respective user accounts are disabled or deleted accordingly.

The NAO observed that the LIS application has an audit trail in place that records amongst others the date and time of who authorised the test, who ordered the test, when the test was printed and on which printer, which workstation was used to carry out these processes etc. Whilst the LIS System administrators can view most of the audit reports, the MITA Health team has elevated privileges to view which users viewed any of the test results.

During the course of the IT audit, the NAO observed that the LIS application offers a reporting functionality whereby a number of reports can be printed once they are *'clinically approved'* from the system. The reports have different styles and sort codes according to where they originate from and are grouped according to the discipline and section. At the time of the audit, the NAO was informed

that there are 18 different types of test reports, but one particular Dynamic Function test requires 22 different test results and the system does not support it. However, the Pathology department managed to find a workaround for this particular test by breaking it in two different reports.

Finally, the NAO was informed that it is envisaged that the current LIS application version 5.8 is upgraded to version 5.9 or 6.0 when the software release is available from the third party supplier. In this scenario, the software release is first installed and tested on the LIS testing environment before it is then deployed on the LIS *'live'* environment according to the Change Management procedures. The same procedures apply whenever there is a hotfix or software patch that needs to be deployed on the LIS *'live'* environment.

3.12 myHealth

Following the publication of an open tender by MITA, for the development and implementation of the myHealth portal[14] in July 2011, a contract was signed between MITA and the preferred bidder, to develop, implement and support the myHealth portal. In this regard, the myHealth portal, which falls under the responsibility of the MEH, was developed and implemented in a phased approach and went live in January 2012. As part of this project, MITA also outsourced the development of a data warehouse specifically designed for the myHealth project. The data warehouse consolidated the patient health data sourced from a number of eHealth systems used by the public health service, which data was then published by the portal using web services.

With the supplier maintenance and support contracts related to the myHealth data warehouse and portal expiring in October 2014 and January 2015 respectively, the MEH took the decision not to renew any of these contracts. Instead, it was decided that MITA should take over the support and maintenance of the current myHealth system to enable more flexibility for the delivery of future additional functionality. In this regard, as from 1st February 2015, this transition of responsibilities from the previous supplier to a development team within the MITA Health team was completed.

During the course of the IT audit, the NAO reviewed how the myHealth portal was being managed and maintained by the myHealth System administrator. The NAO was informed that the myHealth frontend, backend and the publisher websites are accessible over a secure (HTTPS) connection and hosted on the Government's web hosting platform, whilst the backend database is running on a Microsoft SQL Server 2008 platform. Both the frontend and the backend, together with the publisher website, are hosted at MITA-01 Data Centre.

Whilst reviewing the myHealth portal, the NAO observed that myHealth has different web facing endpoints whereby:

- Registered users may view a subset of their personal health data, which currently includes laboratory and medical imaging results, hospital discharge letters and Pharmacy Of Your Choice (POYC) medicines entitlement.

[14] https://myhealth.gov.mt

- Registered users are provided access to information related to their clinical appointments at Government hospitals and Health Centres as well as online facilities whereby they can set up and receive automated e-mail and SMS notifications in addition to reminders for outpatients' appointments.

- Registered users may search and select Doctors of their choice who will be able to view their personal health data. Having said that, Doctors may also register as a patient, in which case they will have access to their own personal health data.

- The myHealth System administrator manages parts of the content of the portal through the myHealth web publisher, whilst the myHealth backend is used to configure certain elements of the portal and to generate and view statistical reports.

The NAO was informed that with the exception of the patients' medicines entitlement records, all the myHealth data is stored and retrieved from a data warehouse. The data in the warehouse is populated from the source applications, such as iCM and ECS, through a number of daily '*extract, transform and load*' (ETL) processes, which are then executed on a periodic basis and involve multiple parties, including third party suppliers. Whilst this method of data acquisition has served the original purposes of myHealth, a number of potential issues were identified through a review carried out by MITA, including issues related to data currency and accuracy. Furthermore, the ongoing maintenance of the data warehouse was very laborious and potentially prone to errors. At the time of the IT audit, the NAO was informed that most of the above issues were resolved after the myHealth data warehouse went through a complete refresh.

As highlighted above, the myHealth portal is accessible over a secure connection. However, to access the myHealth portal, users must have an e-ID account and a password. Thus, a user may register for an e-ID account when applying for the issuance of a new e-ID card at the Identity Management offices in Blata l-Bajda. However, with the mass rollout of renewals of approximately 320,000 ID cards during 2014-2015, most Maltese citizens are already in possession of a new updated e-ID card. Thus, to apply for an e-ID account, one must send an e-mail or visit the Identity Management offices in Blata l-Bajda. In turn, the user would then receive the username and password in the e-mail account submitted upon registration, whilst a unique secure PIN activation code is sent by post to the address as shown on the user's new e-ID card.

Prior to logging on to the myHealth portal, the user must first access the myGov portal[15] to activate the e-ID account. Once an e-ID account is activated, users can select one or more Doctors of their choice, to access their myHealth record, by sending an online request to their desired Doctor/s who in turn may choose to accept or decline such a request. Once the request is accepted, a Doctor-patient link is established and the Doctor may view and release a particular patient's laboratory test results and medical image reports. In this scenario, the user may only view results and reports that have been released by one of their myHealth Doctors. In the meantime, both patients and Doctors retain the ability to cancel a Doctor-patient link at any time.

[15] http://www.mygov.mt

According to statistical information provided by the myHealth System administrator, by the end of 2014, the total number of persons who were using the myHealth portal amounted to 4,042. During the course of the IT audit, the total number of persons who were using the myHealth portal amounted to 4,707. Even though the uptake of persons using the myHealth portal is on the rise, it is still relatively low and can be mainly attributed to the increase in use of e-ID and myGov service subscription. In this regard, the logistical constraints associated with the application process for an e-ID account seems to have discouraged persons from taking the necessary steps to obtain an e-ID. It is however expected that upon completion of the replacement of the now obsolete ID card with e-ID cards, as well as the removal of the myHealth eService subscription, such factors will mitigate the current low up take.

Whilst reviewing the myHealth backend, the NAO observed that this is only used by two System administrators, in order to configure certain elements of the portal, such as SMS or e-mail notification templates. Through the myHealth backend, the System administrator can access the audit logs to view failed or approved user login attempts. The System administrator can also view which Doctor/s was selected by the user and whether a Doctor is still waiting to approve a patient request, or whether a patient request was approved or rejected by their preferred Doctor. All the above logs can then be filtered by the myHealth System administrator and exported to *'.csv'* format.

Through the myHealth backend, the System administrator also maintains the list of registered users and as well as data concerning which users should be flagged as deceased. In this regard, the NAO was informed that every month, the Department for Health Information and Research, within the MEH, forwards by e-mail a list of deceased patients in *'.csv'* or *'.txt'* file format. In turn, the myHealth System administrator uploads the '*.csv*' or *'.txt'* file on the myHealth backend to mark which users are to be flagged as deceased.

During the course of the IT audit, the NAO observed that the myHealth portal has some minor issues, which should be taken into consideration by Management upon reviewing the application. One of the main issues observed throughout the IT audit is that the current myHealth portal is not mobile-friendly. The introduction of Internet enabled mobile devices, such as tablets or smartphones, has raised users' expectations and thus the need of providing services that are both mobile and device independent cannot be ignored. This is especially true in the case of Health professionals whose work often requires a high level of mobility.

Furthermore, the NAO observed that the system does not offer the functionality for parents or guardians to view medical records of children less than 14 years of age under their care. However, individuals over 14 years of age or those who are already in possession of a new e-ID card may submit a request for an e-ID account to be able to view their medical records. The NAO recommends that the Health authorities explore ways how parents or guardians can apply and obtain access to medical records of children under their care. In this regard, if approval is given, the parent or guardian could then select the Doctor of their choice.

Another issue is that as highlighted earlier on, the current myHealth system caters for a limited number of services. Unfortunately, the introduction of new services on this portal is taking too long due to the lack of integration between a number of software applications currently in use within MEH. It is envisaged that the current myHealth system is revamped to become more user friendly and hopefully expand the scope to offer more Health services to the public.

3.13 Online Requisition System

The Online Requisition System (ORS), which was launched around eight years ago prior to the migration of SLH to MDH, was developed by a local third party supplier. The ORS is considered as an extension of the Access Dimensions application, and is mainly used at SAMOC and the Pharmacy department together with the wards and clinical areas within MDH to create requests and order stock items.

Since the ORS is linked to the Access Dimensions application, all the data is retrieved from the same Microsoft SQL database. Thus, as highlighted earlier on in this Chapter, the Microsoft SQL database is divided into two instances. One instance that caters for SAMOC, the Pharmacy, Stores and MM&L departments within MDH, resides on a dedicated Microsoft Windows 2000 server, whilst the other instance, used by the Finance department, resides at MITA's SHE. Although MDH is aware that the Microsoft Windows 2000 server is obsolete and no longer supported by Microsoft, the server hardware is quite old and thus has its limitations. Ideally, the current server is decommissioned and the SQL database is transferred on a virtual environment and hosted at MITA's SHE. Likewise, the NAO was informed that discussions are currently underway with MITA on the possibility of migrating the current setup to Microsoft Windows Server 2012, which would then be hosted on MITA's SHE.

At the time of the IT audit, the ORS was being maintained by one ICT Application officer within the IM&T unit in terms of account management and the provision of first line technical support to the end users within MDH when required. The ICT Application officer also liaised between the local third party supplier and MITA whenever any enhancements, software upgrades or technical assistance is required. If new enhancements to the ORS are required, a request is forwarded to the Director Health Informatics through the Government e-mail. The Director Health Informatics will assess and discuss these requests with the ICT Application officer, and if these new enhancements are deemed in line with the business processes, they are approved and then implemented by the local third party supplier according to the software development lifecycle. The NAO was informed that all the changes are recorded and adhere to the Change Management procedures.

Similarly, the NAO observed that at the time of the IT audit, MDH did not have any written SLAs with the local third party supplier. As a result, when MDH required the assistance of the local third party supplier, the latter provided a service on a time and material basis. However, the NAO was informed that MDH together with the Ministry's IMU (Health) were in the process of finalising an SLA with the local third party supplier.

Whilst reviewing the ORS in terms of user account management, the NAO was informed that whenever a new user requires access to the ORS, their respective Head of department must send an e-mail request to the ICT Application officer. Even though the ORS is linked to the Access Dimensions application, a separate user account is created on the ORS. Upon creation of a new user account, the NAO observed that the passwords are usually created identical to the user login, and that the user is advised to change password upon first logon. In this regard, passwords are only changed upon user's discretion and quite often passwords remain the same as the user's login. Furthermore, the ORS does not offer any password security controls, in terms of password complexity, password expiry, password history or force the user to change password upon first logon. The NAO recommends that the ICT Application officer should liaise with the local third party supplier and verify whether the ORS can be enhanced in terms of password security controls.

In the event that a user has forgotten his/her password, the user must send his/her request to the ICT Application officer through the Government e-mail. A new password is then generated and sent to the user's respective Government e-mail. The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is disabled only if the ICT Application officer is informed by the respective Head of department through the Government e-mail. The same procedure applies for users who are on prolonged leave, career break or maternity leave. In this regard, the NAO recommends that an internal policy is drafted and circulated amongst all staff, stating that whenever a user retires or no longer requires access to the system, the IM&T unit are informed accordingly, and the respective user accounts are disabled.

Furthermore, the NAO was informed that the ORS has an audit trail in place for any failed or successful user login attempts, which are only accessible by the local third party supplier at the back-end, since the ICT Applications officer does not have sufficient access rights to view these logs.

During the course of the IT audit, the NAO interviewed and observed a few users whilst using the ORS. In this regard, the NAO noted that in every department, ward or clinical area, specific users are appointed and granted access to the ORS to order stock items and ensure that the department, ward or clinical area is equipped with the necessary stock items. In ORS, stock items are grouped into five different categories, namely:

- **Conjoints** – stock items of disposable nature used mainly in wards or clinical areas within MDH.
- **Dental** – stock items used specifically at the Dental clinic within MDH.
- **Disposables** – fast moving stock items used across MDH.
- **Infection** – stock items used specifically at the Infection Control unit within MDH.
- **Specials** – specialised stock items used in specific wards or clinical areas within MDH.

Thus, when placing an order, the end user must select a store (Conjoints, Dental etc.), add the necessary items and the amount required. The end user can then view the items selected and modify accordingly before selecting the date when the items are required and whether they must be treated as urgent or scheduled for delivery on a specific date. Once the order is saved, the Nursing officer in charge would then authorise the orders and submit these to the respective stores. The NAO was informed that all authorised requests generated through the ORS are recorded directly in the Access Dimensions application.

The NAO observed that the Supplies department, within the MM&L, liaises between the Stores and other departments, wards or clinical areas within MDH. In this regard, the Supplies department can view the requests of stock items submitted through the ORS and analyse from which department, ward or clinical area the order was received, who submitted the request, who authorised the request and when the order was submitted/authorised. The order would also indicate if the items are needed urgently or requested on a particular date, and the stores from which the items must be retrieved.

The NAO observed that the Supplies department has to login to ORS to view the requests received. The Supplies department would then select every order from the list and vet the order accordingly. Once an order has been vetted, the Supplies department would then print the order and forward the request to the respective Stores department in Microsoft Excel. The Stores department would then handle the requests according to the scheduled dates and deliver the items in the respective department, wards or clinical areas as requested. The NAO was informed that certain clinical wards, such as the Renal unit, are in agreement with the Stores department to deliver items on specific days of the week. Given the above, the NAO noted that the system does not offer any functionality to alert the Supplies department especially when new urgent requests are received. In this regard, the NAO recommends that ideally, an e-mail is automatically sent to the Supplies department whenever a request is marked as urgent or a notification is displayed upon successful logging on to the system.

Furthermore, the NAO was informed that the Stores department have strict instructions to process only requests that are forwarded by the Supplies department. Thus, a clinical area, department or a ward within MDH cannot request the Stores department to deliver a stock item. If certain stock items are needed very urgently, the clinical area, department or ward must go through the Supplies department just the same and raise the request accordingly. The Supplies department would then forward all the requests by e-mail, in Microsoft Excel, since the Stores department does not have access to the ORS. In addition, the NAO observed that all the documentation pertaining to stock items, which were placed on order or are awaiting delivery, are kept separately in folders.

In the event that a stock item does not exist and needs to be added under a specific stores section (ex. Conjoints, Specials etc.), the Supplies department must log on to the Access Dimensions application and input the stock items accordingly. In these circumstances, the Supplies department would update/amend any stock items on the Access Dimensions application only if an authorisation e-mail is received from the respective wards or clinical areas. The NAO observed that whenever a new stock item is inputted into the system, the Supplies department records all the new or amended stock items in a Microsoft Excel worksheet. The latter included details of the stock item, the stock code, the store item under which the stock will be retrieved from and the date when the new stock item or an existing stock item has been inputted/amended in the Access Dimensions application. Any changes made in the Access Dimensions application, is reflected in the ORS when selecting any stock items.

3.14 Online Surgical Register

The Online Surgical Register (OSR) application was developed in-house by an ICT Application officer within the IM&T unit. The scope of the OSR is to key in all the data that is typed in manually on the operating theatre register following any surgical intervention in one of the 33 operating theatres within MDH. With the implementation of the OSR, all the records are kept centrally in a structured database, and can easily be retrieved through a web application.

The NAO was informed that the OSR, which has a Microsoft SQL back-end database and a web application front-end, is hosted at MITA's virtual server environment. MITA is responsible for the daily monitoring and maintenance of the virtual server environment and ensures that the system is backed up regularly. On the other hand, the ICT Application officer provides assistance and user training to operating theatre clerks when required. Furthermore, the ICT Application officer monitors

the Microsoft SQL database, in terms of error logs, storage, and backups amongst others, offers first-line technical support and assists the operating theatre clerks whenever new functionality is required.

The NAO noted that the OSR application is accessible through a login and a password and at the time of the IT audit, the OSR application had around 106 active user accounts. The NAO was informed that passwords are not stored in clear text and the OSR application has a password complexity rule in place, whereby the password must be set with a minimum of eight characters in length and must include a mix of letters and numbers. However, the NAO observed that passwords do not expire, old passwords can be re-used, and the system does not block access after a particular amount of unsuccessful logon attempts. The NAO is of the opinion that the OSR application should adhere to password management best practices whereby the password history rule should at least be implemented, whilst passwords should be made to expire after a stipulated number of days.

In the event that a user has forgotten his/her password, the user must send his/her request to the ICT Application officer through the Government e-mail. A new password is then generated and sent to the user's respective Government e-mail. The NAO was informed that whenever a user retires or no longer requires access to the system, the user account is disabled. The same procedure applies for users who are on prolonged leave, career break or maternity leave. However, in every circumstance, user accounts are only disabled as long as the Nursing officer in charge or the user him/herself informs the ICT Application officer through the Government e-mail.

The NAO observed that whenever a new user account is created on the OSR application, the ICT Application officer would either assign a *'normal'* user role, whereby the user could create and view records within the designated operating theatre group, or else assign a *'Data Management Unit'* user role. The latter is only granted to users within the DMU to clinically code all the data retrieved from the OSR according to the international statistical classification - ICD-9 codes. Apart from these two user roles, the OSR application has an *'administrator'* user role, which is only used by the ICT Application officer, for the overall management of the OSR application and to provide one-to-one user training when required.

During the course of the IT audit, the NAO was informed that the OSR application has an audit trail in place, logging any failed or successful user login attempts, and which is only accessible by the ICT Application officer at the front-end.

The OSR application offers a reporting functionality whereby the operating theatre clerk can only issue a report pertaining to the assigned operating theatre group. In other words, the operating theatre clerk can only view the data that has been inputted according to the assigned operating theatre group. Once the start date and end date are selected, a detailed report is generated from the OSR application and viewed in Microsoft Excel.

Finally, if new enhancements to the OSR application are required, a request is forwarded to the Director Health Informatics through the Government e-mail. The Director Health Informatics will address these requests with the ICT Application officer, and if these new enhancements are deemed fit, they are approved and implemented according to the software development lifecycle. The NAO was informed that all the changes are recorded and adhere to the Change Management procedures.

3.15 Overall recommendations

Most of the IT systems reviewed during the course of the IT audit are integrated with the CPAS application. However, the NAO observed that a few other software applications, such as the DCU application, are not integrated with CPAS to retrieve patient demographics.

The NAO recommends that such software applications are integrated with the CPAS application, thus avoiding any inconsistencies in patient's demographics and eliminating the duplication of work in maintaining such data on both CPAS and the IT systems in use within MDH.

Furthermore, MDH should develop an IT strategy to promote the further integration of IT software applications within MDH and the possible integration with Government Corporate databases, such as CdB, to retrieve patient demographics.

With regards to software applications, which were developed in-house, MDH should also take the necessary precautions to ensure that a final working version of the source code of the above applications and the respective technical manuals are available to Management and held in a secure location.

Chapter 4

Information Security

Chapter 4

Information Security

Information security refers to the processes and methodologies, which are designed and implemented to protect Information Systems and any confidential, private and sensitive information or data from unauthorised access, misuse, disclosure, destruction, modification or disruption. An information security breach includes amongst others a network disruption due to a Denial of Service (DoS) attempt or Information Systems infected by malicious software, such as malware, with the consequence of allowing third parties to gather sensitive information or gain unauthorised access to computer systems and the data therein.

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

The NAO verified whether MDH adheres to the GMICT and internal security policies and procedures to maintain the confidentiality, integrity and availability of data.

4.1 Security Management

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

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

4.1.1 Information Classification

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

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

At the time of the IT audit, the NAO was informed that MDH does not have an official information classification policy but have drafted an internal *'Information Sensitivity policy'.* The latter intends to follow the GMICT Information Security policy[16], which is in line with ISO 27001:2013 and encompasses various aspects of security, including guidelines on how to protect the confidentiality of information by preventing unauthorised disclosure of data. In this scenario, to protect the confidentiality of information, data can be classified under different security levels:

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

Depending on the level of classification, one should control the level of clearance needed to view such information, and how it must be stored, transmitted and destroyed. In this regard, the NAO recommends that this internal policy should be disseminated amongst MDH employees and ensure that everyone adheres to this policy.

[16] https://mita.gov.mt/en/GMICT/Pages/Security.aspx

4.1.2 Retention and Storage of Data

A data retention and storage policy defines how an organisation deals with maintaining its information. Such policy establishes a pre-determined set of time frames according to which an organisations retains the information collected. Furthermore, this policy includes the procedures for archiving the information, guidelines for destroying the information when the specified time limit has been exceeded, and the special mechanisms that are applied for handling the information when under litigation, such as lawsuits or criminal investigations.

During the course of the IT audit, the NAO noted that MDH holds considerable amount of personal data, which is mostly retained in patients' medical files and are physically stored at the Medical Records department. In this regard, the NAO was provided with a copy of the *'Personal Clinical Patient Data (Medical Records): Retention and Disposal Policy for Malta',* which stipulates that the *"...Medical Records in Malta should be kept for a patient's lifetime, and thereafter have a minimum retention period of 10 years after death."*

Furthermore, the above policy stipulates that "*Once their retention period expires, patient medical records should be appraised and transferred to the National Archives, or destroyed. The need to retain records further or permanently preserve them will depend on their long-term wider epidemiological, medical, research or historical value*."

Apart from the above policy, MDH should follow the *'Retention Policy for HR documents*[17]*'* that was issued by the Data Protection unit in conjunction with PAHRO, and which all Government departments need to abide with. Furthermore, MDH also adheres to the Data Protection Act 2001, Chapter 440 of the Laws of Malta, and the related Legal Notices, whereby the processing of personal data must be:

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

4.1.3 Disposal of Information

Information Systems store data on a wide variety of storage media, including internal and external hard disks, flash memory such as memory cards or USB pen drives, optical storage media such as CDs or DVDs and other types of removable media such as tapes or cartridges. Data can also be presented in

[17] https://issuu.com/nationalarchivesmalta/docs/hr_retention_policy_april_2012

printable format. To prevent unauthorised access, it is critical that data be rendered unreadable when documents or the drive on which data resides are no longer needed. Thus, any confidential electronic and paper information must be disposed of securely to minimise the risk of unwanted disclosure.

If confidential information is disclosed or lost, this could cause harm or distress. This includes personal sensitive data as defined by the Data Protection Act.

As highlighted above, since MDH holds a considerable amount of personal data, which is mostly retained in patients' medical files, and in order to maintain patient confidentiality at all times, hard copies of patients' medical records should be destroyed by shredding or incineration. In addition, CDs, DVDs, hard disks and other forms of electronic data storage should be overwritten, securely wiped or physically destroyed.

The NAO observed that from time to time, MDH users are reminded through internal memos, not to save any documents on a PC or laptop's hard disk, but rather to store the data on the MDH network drive, so as to ensure that no data is lost in the event of a hardware malfunction. In addition, the IT Support unit within the IM&T unit is not responsible to back up any data that is stored locally whenever a PC or laptop will be disposed off or transferred to another user. In this scenario, the NAO observed that the IT Support unit would format the hard disk and re-install the PC or laptop's hard disk using a software image provided by MITA, in the event that the PC or laptop is transferred to another user. In this regard, the NAO is of the opinion that the IT Support unit should securely erase all the data residing on the hard disk, using a data wiping software application, irrespective of whether the PC or laptop is to be disposed off or transferred to another user. This would ensure that the original data cannot be recovered from the hard disk.

Furthermore, the NAO recommends that MDH should ensure that the disposal of information on all types of electronic media should follow the same procedure. As a result, a policy should be drafted and communicated internally describing the procedure that should be adopted for the disposal of any confidential information, which may reside electronically on flash memory devices, CDs, DVDs, etc., through shredding, secure wiping and/or physical destruction accordingly.

4.1.4 Backup and Recovery of Data

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

The NAO observed that the IM&T unit have drafted a *'Backup Retention and Archive Policy'* to establish the structures that exist around the management of data in terms of backups, retention and retrieval of data, documents and digital content held at MDH and SAMOC.

During the course of the IT audit, the NAO noted that the IM&T unit have six NAS devices installed at the MDH server room, of which only four devices are currently operational. Whilst two NAS devices are used to store data pertaining to all the users at MDH and SAMOC, the other two NAS devices are

used for backups. Thus, one of the NAS devices has been configured to store *'live'* backups, whilst the other NAS device has been configured to replicate all the *'live'* backup files in the early hours of the morning, to ensure that the IM&T unit have a fallback in the event that the primary NAS device used for the *'live'* backups malfunctions. Apart from the MDH and SAMOC users' data, the Dakar application and other MDH applications hosted on virtual environments at the MDH server room are also being backed up on the NAS devices.

As highlighted earlier in the report, the Networks team within the IM&T unit were responsible for the implementation of system backups and restore processes. These tasks include the overseeing of the actual backup, establishing that the NAS devices are operational, that all the data is being replicated from one NAS device to another and ensuring that the backups are valid and available for restore when required. As highlighted earlier in the report, at the time of the IT audit, both officials manning the Networks team resigned from MDH and instead a few ICT Application officers within the IM&T unit were entrusted with the management of the backups, and the retention and recovery of data.

During the course of the IT audit, the NAO noted that a dedicated backup software application was installed and configured to manage all the backups and recovery of data. Whilst reviewing the backup process, the NAO observed how the ICT Application officers ensure that the daily/weekly/monthly backup has been completed successfully. In this regard, the backup software application has been configured to alert the ICT Application officers through an e-mail notification, which is sent automatically, when a backup has failed or has been completed successfully. In the event that a scheduled backup fails to complete, the ICT Application officers must establish the root cause of failure, and decide whether a manual backup should be taken.

In addition, the NAO was informed that the daily backups are retained for two weeks, to cover for and protect against widespread loss or to allow recovery from data corruption. The backup is then deleted when the retention period expires, whereby the oldest backup file is removed manually. On the other hand, the weekly backups are retained for up to 13 weeks. If weekly backups are required to be stored for more than 13 weeks, a business case must be presented to the IM&T unit along with the necessary authorisation. Apart from the daily and weekly backups, critical applications, such as the Dakar application, have monthly and yearly backups, in which scenario the monthly backups are retained for two years whilst the Dakar yearly backup has been retained since 2007.

In the meantime, most of the software applications selected for the purpose of this IT audit are hosted at MITA's SHE. The NAO was informed that most of these software applications are backed up according to the *'grandfather-father-son'* backup rotation, whereby an incremental backup to disk is scheduled on a daily basis, whilst a full system backup is scheduled weekly or monthly and stored on MITA's storage environment. As part of MITA's Hosting Services Contract, in the event that a backup process fails to complete, the Network Operations Centre within MITA would inform the relevant stakeholders accordingly. Meanwhile, to ensure that the data can be fully restored from the backup files, a random test restore from a pool of backup files is carried out by MITA every quarter.

4.2 Identity and Access Management

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

4.2.1 Authentication

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

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

During the course of the IT audit, the NAO observed that all the requests for the creation, modification or deletion of user accounts to access the CORP Domain, the Government e-mail and Internet, Corporate systems (such as CdB or DAS) or critical Health systems hosted at MITA (such as iCM, LIS, RIS and PACS) must be submitted through a *'Request for IT Service form'*, which must be filled in and signed by the relevant stakeholders. Most of these *'Request for IT Service forms'* are submitted to the IT Services Support team within the IM&T unit to raise the necessary eRFS with MITA's Service Call Centre. After processing these requests, MITA would either forward the user login and password to the IT Services Support team or else forward the request to the respective ICT Application officer or System administrator for the creation, modification or deletion of a user account and to grant or revoke access rights accordingly.

On the other hand, all the requests for the creation, modification or deletion of user accounts to access Health applications, which were developed locally and are being maintained in-house, such as the ECS or ORS applications, must be submitted through the Government e-mail. The Nursing officer or the Head of department must endorse these e-mail requests and forward them to the respective ICT Application officer. The latter would then create, modify or delete a user account and grant or revoke access rights accordingly.

Whilst most of the user accounts are created according to the standard naming convention adopted by MITA across Government departments, the NAO observed that the user accounts on the Access Dimensions application do not adhere to a standard naming convention and are thus being created haphazardly. In this regard, the NAO is of the opinion that the ICT Application officer together with the local third party supplier should review the *'user records'* and ensure that the *'user id'* and the *'name'* fields should follow a standard naming convention.

In the meantime, whenever a user retires or no longer requires access to the system, the NAO was informed that the user account is disabled only if the ICT Application officer is informed through the Government e-mail. A similar procedure is applied for users who are on prolonged leave, career break or maternity leave, whereby the user account is disabled until the user returns to work. In this regard, the NAO recommends that an internal policy is drafted, which clearly indicates that whenever a user retires or no longer requires access to the system, the IM&T unit are informed, and the respective user accounts are disabled or deleted accordingly.

Finally, the NAO observed that in Q1 2015, MDH had triggered a process to verify whether there are any inactive user accounts, which need to be deleted. In this regard, MITA had compiled a report of all the active and inactive Domain user accounts and forwarded it to MDH to take the necessary actions. In turn, if a Domain user account is marked as inactive, the IT Services Support team would carry out various checks with different stakeholders to establish whether an active or inactive Domain user account needs to be retained, before raising an eRFS with MITA for the deletion of the respective user account. Whilst the NAO commends this initiative in the management of Domain user accounts, the NAO recommends that this should be on-going and rather than a one-off exercise. Furthermore, once it has been established that a Domain user account is no longer in use and needs to be deleted, the same procedure should be applied to all the software applications in use within MDH whereby the ICT Application officer or System administrator must delete the respective user account.

4.2.2 Password Management

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

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

During the course of the IT audit, the NAO observed that whilst blank passwords are not allowed, most of the IT software applications selected for the purpose of this IT audit including Access Dimensions, CPAS, DCU and Dakar amongst others, do not adhere to password management best practices. In this regard, these IT software applications do not offer sufficient password security controls, in terms of password complexity, password expiry, and password history, nor do they force the user to change the password upon first logon.

In this regard, the NAO is of the opinion that those IT systems that do not offer sufficient password security controls, should be enhanced and adhere to the GMICT Password policy[18].

In the meantime, at the time of the IT audit, the NAO was informed that the ICT Application officers within the IM&T unit maintain a list of both previous and current local administrator passwords of servers hosted at the MDH server room in a Microsoft Excel worksheet. Access to the latter is protected with a password and restricted to a limited number of ICT Application officers within the IM&T unit.

[18] https://mita.gov.mt/en/GMICT/Pages/Security.aspx

In this regard, the NAO is of the opinion that in order to ensure that this worksheet is kept secure at all times, the ICT Application officers should consider either implementing file or folder encryption.

Furthermore, the NAO was informed that since most of the IT software applications selected for the purpose of this IT audit are being administered by an ICT Application officer, every administrator password is being stored separately in a sealed envelope. The latter are securely kept under lock and key by the Director Health Informatics. In the absence of an ICT Application officer, if an administrator password is required, a new password is generated, after the securely stored password has been used, and is then stored in a sealed envelope. In this scenario, the NAO is of the opinion that whenever a new password is generated, the sealed envelope should be signed by the Director Health Informatics and the officer who retrieved the administrator password, and should also specify the date when the password was changed.

4.2.3 Auditing

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

During the course of the IT audit, the NAO observed that most of the IT software applications selected for the purpose of this IT audit have audit trails in place to record amongst other the successful or failed login attempts according to the date and time, and who created, modified or deleted data on that particular software application. Similarly, the audit logs on servers and NAS devices hosted at MDH server room were configured to record login/logout activity and operating system activity in the Security log. The latter is one of the primary tools used by the ICT Application officers or System administrators to detect and investigate attempted and successful unauthorised activity on servers or NAS devices and to troubleshoot any problems that might arise.

In the meantime, as highlighted in the previous Chapter, the NAO was informed that the Dakar application does not offer any audit trail functionality, since the latter was disabled as it was generating too many logs, which affected the performance of the Dakar application. Thus, MDH cannot currently quantify when and who accessed, inputted, modified or deleted data from the Dakar application. The NAO recommends that the key stakeholders within MDH together with the local third party supplier should review the current Dakar application and server specifications and come up with a solution to re-enable the audit trail functionality without impacting the use of the Dakar application by the end user.

4.3 Security Awareness and Training

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

The NAO observed that MDH users are regularly notified by MITA, through the Government e-mail on any security issues. In addition, the IM&T unit publishes circulars on the KURA portal every now and then, to inform MDH users on any security issues. However, the NAO believes that security awareness should be ongoing, whereby users are provided regular updates to foster security awareness and compliance with security policies and procedures within MDH. In this regard, the NAO recommends that the IM&T unit should draft a set of computer security guidelines for all the users within MDH with the aim of:

- informing MDH users how to protect their workstations and their personal information by using the shared folder structure on the MDH network rather than saving work-related files locally and how to backup any important files and offline mailboxes;

- informing MDH users about the security risks of the Internet, and highlight the appropriate actions that should be taken to minimise those risks;

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

- providing tips on how to safeguard passwords, and prohibit the sharing of logins and passwords.

The NAO recommends that security awareness should be offered as part of the induction sessions given to new employees within MDH, and should also be part of an ongoing programme that seeks to ensure that all the users are familiar with the information security policies and best practices that govern the use of IT assets.

Finally, as highlighted earlier on in the report, the IT Training section within the IM&T unit, offers one-to-one or group training sessions on the major software applications in use within MDH, including the ECS, iCM, and PACS applications. The NAO also observed that in certain areas, MDH adopted the *'train-the-trainer'* approach, whereby the System administrator or key persons are offered specialised training. In turn, these officers would then disseminate the information and offer on-the-job training to other users within their respective ward or section. This is the case of the CPAS team, who offer on-the-job training or schedule refresher courses to users from time-to-time. However, whilst reviewing some of the software applications selected for the purpose of this IT audit, the NAO observed that certain users were not confident in using the system. The NAO recommends that users should be encouraged to raise these issues with their superiors and request that refresher courses or specialised training are offered on a regular basis.

4.4 Anti-Virus Software

To effectively control and prevent the spread of malware, any department or entity should implement a reliable Anti-virus software across its network infrastructure. The NAO observed that the PCs and laptops at MDH are installed with an Anti-virus software application as part of the Government standard software package. Additionally, the Anti-virus software application installed on all the PCs and laptops,

which are connected to the MDH network infrastructure, are being managed by MITA, whereby any Anti-virus updates or urgent fixes are pushed automatically over the Government network.

Similarly, even though the MDH IT systems that are hosted on MITA's SHE have a different Anti-virus software package installed from that installed on the MDH PCs and laptops, the former are also being managed by MITA and are thus being updated daily with the latest virus definitions over the Government network.

In the meantime, the NAO was informed that MITA utilizes a tool that provides a reporting mechanism on the services that it offers, including Anti-virus configurations and Patch Management services. This reporting tool is mainly used for PCs and laptops since MITA has a different processing mechanism in terms of servers' monitoring. In addition, the NAO was informed that MITA has granted access to this reporting tool to the Ministry's IMU (Health), at a Ministerial level. Thus, the reports generated from this tool must be filtered at departmental level when extracted. Even though MITA remains responsible for checking for any anomalies and the reports generated are highly technical, the Ministry's IMU (Health) must seek MITA's assistance if in doubt on any anomalies highlighted in any of the reports.

Finally, during the course of the IT audit, the NAO observed that whilst the PCs and laptops are being updated automatically, the Anti-virus software application installed on the Dakar server hosted at MDH server room was found to be disabled. Since the recently appointed ICT Applications officers were not aware why the Anti-virus software application was disabled, this matter was raised with the local third party supplier to verify whether the Dakar application would be effected if the Anti-virus software application is re-enabled.

4.5 Patch Management

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

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

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

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

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

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

To mitigate any risks related to malware and security exploits, the NAO was informed that MDH adopts two different approaches when applying patch management on servers and workstations. In this regard, the NAO observed that the PCs and laptops within MDH are configured to automatically download and install product updates over the network. These product updates are being managed by MITA whereby hotfixes and security patches released by Microsoft are distributed across the MDH network infrastructure. These are then downloaded and installed automatically on all the PCs and laptops within MDH.

On the other hand, the NAO observed that a different approach is being adopted within MDH on how these hotfixes and patch releases are installed on servers. In this regard, the NAO was informed that the local third party suppliers must approve most of the product updates before they are installed manually on the testing environment. If no abnormal behaviour is observed, these hotfixes and patch releases are then deployed on the *'live'* servers. However, at the time of the IT audit, the NAO noted that the Dakar server hosted at MDH server room was not being updated with any hotfixes or patch releases. In this regard, it transpired that the last hotfix or patch release was installed in 2014. Once again, since the ICT Application officers were not aware that the Dakar server was not being updated with any Microsoft Windows hotfixes or patch releases, the matter was raised with the local third party supplier to discuss how to proceed with these installations, and ensure that the Dakar server is constantly updated with the latest hotfixes and patch releases.

Chapter 5

IT Operations

Chapter 5

IT Operations

5.1 Security Controls

Security controls are technical or administrative safeguards or countermeasures to avoid, neutralize or minimize security risks to physical property, information, computer systems or other assets within the building. In this regard, the NAO reviewed whether physical and environmental access controls are in place to safeguard all the data and IT assets within MDH.

5.1.1 Physical Access Controls

Information security incidents may occur if unauthorised users gain access to sensitive information by defeating physical access control mechanisms. Therefore, having a sound physical access control mechanism in place would determine who, where and when an individual is allowed to enter or exit and at the same time protect the computer hardware, software, and network equipment from damage, theft and unauthorised access.

During the course of the IT audit, the NAO interviewed a number of users and reviewed the physical access control mechanisms at the MDH Server room and across MDH. In this regard, whilst auditing the MDH server room, the NAO observed that the room is accessible only to a restricted number of users within the IM&T unit through the use of an ID Tag system and a key. In the event that maintenance is required on the environmental controls or on the hardware equipment installed inside the room, the NAO was informed that one of the authorised users within the IM&T unit accompanies the technician or engineer. Furthermore, the NAO observed that the MDH server room has a visitors' logbook in place, whereby users sign in and clearly indicate the date, time of entrance/exit, name and surname, company and the purpose of their visit.

In the meantime, the NAO was informed that if the MDH control room was alerted with a fire alarm and emergency access to the MDH server room is required after office hours, the Director Health Informatics is informed by the Security officer prior to entry and updated accordingly.

Whilst reviewing the MDH server room, the NAO noted that a Closed-Circuit Television (CCTV) camera is installed in the corridor and directed towards the door of the MDH server room to record individuals who gain access to this room.

In this regard, surveillance systems, such as CCTV cameras, mitigate the risks of undetected physical intrusion by serving as a detective control as well as a deterrent for would-be intruders. The absence of these systems would increase the risk of theft and other criminal activities. At the time of this IT audit, the NAO was informed that MDH has around 125 CCTV cameras installed across MDH, some of which are purposely not operational. Furthermore, MDH has another 24 portable CCTV cameras, which are normally used for investigation purposes. The NAO noted that wherever a CCTV camera is installed, irrespective of whether it is operational or not, a clear sign is placed prior to entering that particular area within MDH, to inform the individual that a CCTV camera is monitoring the area.

All the CCTV cameras are managed by the Engineering department within MDH and monitored by a third party security firm, which was entrusted with the overall security of the MDH premises, from the MDH Control room. In this regard, the NAO was informed that the MDH Control room captures all the CCTV footage and stores it on dedicated PCs for five days. In addition, all the CCTV footage is encrypted and kept on dedicated hardware at the Engineering department within MDH for a two-month period. After the lapse of this period, the CCTV footage is automatically deleted and overwritten by new video footage.

If a video footage needs to be retrieved from a particular CCTV camera on a specific date and time, the local third party security firm must type in a password to retrieve and view the CCTV footage. The NAO noted that the password should be changed upon use and a new password generated, which should be kept in a sealed envelope as part of the third party security firm's policies and procedures. In this regard, the NAO commends the number of security policies and standard operating procedures the MDH Control room has in place. The NAO noted that these are continuously being updated, printed and kept in physical files.

The capturing and recording of images by means of a CCTV camera, leading to the identification of a person, constitutes processing of personal data. Therefore, by definition, this processing falls within the parameters of the Data Protection Act. In this regard, if the local third party security firm retains the images on behalf of MDH, the latter is obliged to govern the relationship by means of a legally binding agreement. The agreement must specify that the local third party security firm shall only act upon the instructions of MDH and shall implement all the necessary technical and organisational safeguards against accidental and unlawful forms of processing.

Like any other hardware equipment, all the CCTV cameras are covered by a hardware maintenance contract, which was awarded to a local third party supplier for the provision and maintenance of the physical and environmental access controls within MDH. In this regard, the NAO was informed that the local third party supplier must maintain all the CCTV cameras installed. This entails the cleaning of the CCTV camera lenses, checking for any wear and tear of cables, testing the battery backup and ensuring that every CCTV camera is sharply focused and free from any distortion/interference. Once the local

third party supplier certifies that the CCTV cameras are in good working order, the NAO was informed that the Engineering department are free to carry out a number of random audits and quality checks on any of these CCTV cameras.

As highlighted earlier in the report, MDH has around 30 network cabinets, which are managed by MITA. However, of these 30 network cabinets, the IT Technical Support team within the IM&T unit, can only access 28 network cabinets whenever they need to patch network points and connect IT equipment to the MDH network, whilst the remaining two can only be accessed by MITA. The Network rooms, where every cabinet is installed, are securely locked, and the IT Technical Support team must sign for the key at MITA's Network Operations Centre within MDH, whenever they need to access a particular Network room.

Finally, all MDH and non-MDH employees, who are providing a service within the MDH premises, are presented with an ID Tag. The latter is also configured by the Identification Cards office to grant access to MDH and non-MDH employees to specific areas or wards within MDH. Furthermore, every ward or area within MDH is physically manned by a Security officer from within the local third party security firm, to make sure that no unauthorised users are allowed in wards or areas, and to instil a safe environment for all patients and staff within MDH.

5.1.2 Environmental Access Controls

Environmental exposures are due primarily to naturally occurring events such as flooding, fire, lightening, power failures and other environmental disasters and thus should be given the same level of protection as any physical exposures. In this regard, the NAO examined the types of environmental access controls that exist within MDH and the measures being taken to mitigate the above-mentioned risks.

Whilst reviewing the MDH Server room, the NAO observed that the room is equipped with an air-conditioning unit and a water-based fire suppression system, which are monitored by the Engineering department and maintained by the respective local third party supplier. In addition, the ICT Application officers within the IM&T unit also carry out a visual inspection on a daily basis to ensure that the temperature inside the room is kept constant and that all the equipment is up and running.

Furthermore, the MDH Server room is also equipped with a smoke detector that is connected to a central fire alarm system at the MDH Control room. Thus, if any smoke is detected inside the room, the MDH Control room will be alerted with an audible alarm and a Security official is sent on site to inspect the area.

Similarly, the Network rooms where the network cabinets are installed, are also equipped with an air-conditioning unit, a water-based fire suppression system and a smoke detector. However, the NAO noted that neither the MDH Server room nor the Network rooms are equipped with any raised flooring. One of the main benefits in having raised flooring is that it prevents from flooding caused by external environmental factors or even something as simple as a broken pipe from the air-conditioning unit for instance, thus reducing damage to equipment installed on the floor. In view of the fact that at the time of the IT audit the MDH Server room had two floor-mount UPSs and a server installed next to the server cabinet, whilst both the network cabinet and the server cabinet are installed very close to

the air-conditioning unit, having a raised flooring might be an option. Alternatively, the NAO is of the opinion that the equipment found at the MDH Server room is elevated from the floor and placed on rack-mounted shelving for instance.

During the course of the IT audit, the NAO noted that MDH is equipped with a number of fire extinguishers, which are installed in strategic areas within the building and are inspected and serviced annually by a local third party supplier.

Furthermore, the NAO observed that the equipment installed at the MDH Server room and the Network rooms is connected to a UPS to safeguard all the IT components from any power surges or unexpected shutdowns. Furthermore, the NAO noted that since most of the servers installed inside the MDH Server room have dual power supplies, all the servers are connected on to different UPSs. Thus, in the event of a hardware malfunction on one of the UPSs, the servers will remain switched on, as the load will be shifted on the remaining UPS. However, due to its criticality, MDH is backed up by diesel-powered generators, which are regularly monitored and tested by the Engineering department, in the event of an unexpected power failure. In this regard, the NAO was informed that every month, the Engineering department simulates a power failure in certain areas within MDH, to ensure that the power generator kicks in whenever there is an unscheduled power cut. During this simulation, the IM&T unit are on stand-by in the event that any of the IT equipment installed inside the MDH Server room shuts down unexpectedly.

Finally, the NAO was informed that it is envisaged that most of the servers and the NAS devices will be migrated to MITA's SHE. However, the IM&T unit plan to retain the MDH Server room and intends to use some of the current servers for testing and storage purposes. In this regard, the NAO was informed that the IM&T unit were looking into the possibility of replacing the water-based fire suppression system with a gas-based (FM-200) fire suppression system.

5.2 IT Service Management

IT Service Management (ITSM) is a general term that describes a strategic approach for designing, delivering, managing and improving the way IT is used within any organisation. The goal of every ITSM framework is to ensure that the right processes, people, and technology are in place so that the organisation can meet its business goals. As a result, the ITSM framework employs the Information Technology Infrastructure Library (ITIL)[19] that provides best practices for aligning IT with business needs. During the course of the IT audit, the NAO assessed whether MDH adheres to the ITSM best practices, which provide assurance that the expected level of service is being delivered within MDH.

Incident management can be defined as one of the critical processes in the ITSM framework. The first goal of the incident management process is to restore a normal service operation as quickly as possible and to minimise the impact on business operations, thereby ensuring that the best possible levels of service quality and availability are maintained. It is thus essential for any incident handling process to prioritise items after determining the impact and urgency.

[19] https://www.axelos.com/best-practice-solutions/itil

As highlighted earlier in this report, even though the IM&T unit act as a point of reference between the MDH end users, MITA, and local third party suppliers, the end users are advised that whenever any technical assistance is required, they should contact MITA's Service Call Centre. The latter would raise an incident request in their Call Logging System and escalate the incident request to the respective teams within the IM&T unit. However, whilst reviewing the software applications selected for the purpose of this IT audit, the NAO observed that certain users phone the ICT Application officers directly whenever they require assistance. In this scenario, since these calls are not being logged through the proper channels, the IM&T unit cannot quantify exactly the number of incident requests that were serviced periodically, and whether the incidents are repetitive or correlated to identify and solve the root cause of the problem. Furthermore, if all the incident requests are registered through the proper channels, the IM&T unit could substantiate the level of support being provided within MDH, which would even help in devising human resources capacity planning and decision-making. In this regard, the NAO recommends that a memo is issued and circulated within MDH, guiding the users to use the proper channels when logging calls for assistance related to IT systems.

Problem management should aim to reduce the adverse impact of incidents and problems that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. Thus, once a problem is identified and the analysis has determined the root cause, the condition becomes a *'known error'*. A workaround can be developed to address the error state and prevent future occurrences of the related incidents.

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

During the course of the IT audit, the NAO observed that both the ICT Application officers and the third party suppliers adhere to a Change Management procedures, whenever a new enhancement, functionality or a software fix is implemented. This is achieved by formalising and documenting the process of a change request, obtaining a written authorisation, which is usually sent through the Government e-mail, carrying out the necessary testing in a server-testing environment, implementing the change request and finally informing the respective users when the change is completed.

Furthermore, most of the software applications selected for the purpose of this IT audit are hosted on either MITA-01 Data Centre in St. Venera or at MITA's MDH Data Centre. As a result, MITA would notify all the relevant stakeholders with a plan for the implementation of any changes, which may affect the server or virtual environment where the software application is hosted. However, these changes may be delayed by MITA to allow the third party supplier to take remedial action as necessary to ensure that the proposed changes do not have any impact on the system. On the other hand, MITA reserves the right to proceed with the implementation of the changes and inform the relevant stakeholders if the changes required are deemed by MITA to be of a critical nature.

5.3 E-mail and Internet Services

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

In this regard, since MDH's e-mail and Internet services are provided by MITA through the Government's communications backbone, known as MAGNET, the NAO was informed that MDH adheres to the *'Electronic Mail and Internet Services Directive'*[20] that was issued by the former Central Information Management unit (CIMU) in 2003.

The NAO was informed that almost every user within MDH is provided with an e-mail and Internet account. The directive highlighted above stipulates that the e-mail service is provided for official business use only and is deemed the property of the respective Government department. Thus, an e-mail, including attachments, that is created, sent, received or printed via the Government e-mail service, becomes the property of MDH. Moreover, the personal use of e-mail is allowed only in exceptional cases, and provided that this does not interfere with the performance of the account holder's duties or those of other account holders.

Similarly, every user is responsible and held accountable for Internet activities executed. Thus, every MDH user who owns an Internet account must also abide with the above directive. Even though an adequate filtering technology is being used by MITA to prevent access to illegal material, every MDH user should ensure that his/her account remains secure and should not disclose the password or use someone else's password.

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

At the time of the IT audit, the NAO was informed that MDH has around 617 generic e-mail accounts, which are managed by specific end users within MDH. As a result, all end users, who have been granted access to these generic e-mail accounts, should ensure that the respective mailbox is properly maintained in terms of e-mail correspondence, mailbox size and the storage of offline mail. Furthermore, the NAO observed that offline mailboxes of personal or generic e-mail accounts are being stored locally on the end users' PC or laptop hard disk. Since the end users are not allowed to store offline mailboxes on the MDH shared network drives, the NAO recommends that the IM&T unit should provide guidelines to all the end users within MDH on how to backup and securely store offline mailboxes.

[20] https://mita.gov.mt/en/GMICT/Pages/Email--Internet-GMICT-Policies.aspx

Finally, the NAO is of the opinion that the IM&T unit should draft an internal policy and periodically remind all the MDH users who own an e-mail or Internet account, about the salient points highlighted in the *'Electronic Mail and Internet Services Directive'*, especially the restrictions on use of e-mail and Internet services as reproduced in Appendix D.

5.4 Web Filtering

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

MITA, being the Government Internet service provider, has adopted the *'Web Filtering Directive'*[21] that was issued by the former CIMU in 2003. The aim of this directive is to set up methods for controlled access to Internet websites based on Government needs. The directive addresses the legal risk to Government and the productivity of Government Internet account holders.

Finally, the web filtering can be configured to either *'whitelist'* or *'blacklist'* a website. Websites found in the *'whitelist'* group can only be accessed when *'whitelist'* is enabled. On the other hand, if *'blacklist'* is enabled, the web filter will allow all websites except those listed in the *'blacklist'*. In the event that a particular website is being blocked or needs to be blocked by the web filter, the IM&T unit would liaise with MITA's Service Call Centre to take the necessary action to *'whitelist'* or *'blacklist'* the website accordingly.

5.5 Internal and External Communications

Organisations cannot operate without communication. Communication can take various forms but these all involve the transfer of information from one end to another. Just like any other organisation, MDH strives to disseminate information both internally and externally. In this regard, during the course of the IT audit, the NAO reviewed the different means of communication that are at the disposal of the MDH users, Health entities and the general public, namely the MDH website, the official MDH Facebook page, the MDH portal and KURA.

5.5.1 KURA

KURA, which was launched in 2004, is the main hospital portal for MDH, SAMOC and Karin Grech Rehabilitation Hospital, and whilst it is currently being maintained by the Ministry's IMU (Health), it is being hosted by a local third party supplier.

The purpose of the KURA portal is to serve as an internal communication and information dissemination platform to encourage online collaboration between different staff users. In this regard, KURA

[21] https://mita.gov.mt/en/GMICT/Pages/Email--Internet-GMICT-Policies.aspx

offers a number of facilities, whereby hospital staff can read important news, download and print forms, circulars, publications, standard operating procedures, rosters, articles related to Continuing Professional Development, and many others.

The NAO observed that whilst most of the above can be accessed over the Government network, if an MDH user wishes to make use of the services offered by KURA, the user must submit a '*Registration Request Form'* from the KURA portal. The ICT Applications officer within the Ministry's IMU (Health) would vet all the registrations submitted online before a user account is created on KURA. The user account credentials are then sent to the respective user through KURA's generic e-mail, which is also maintained by the Ministry's IMU (Health). In the meantime, users are expected to submit any requests for assistance to KURA's generic e-mail. Thus, authorised users may request that the news section is updated or else a new or an existing policy, form, standard operating procedure etc., is updated and uploaded on to KURA. In this regard, the NAO observed that the ICT Applications officer references all the documents received in a Microsoft Excel worksheet before they are uploaded through the Content Management system provided by the local third party supplier.

Meanwhile, the NAO was informed that the '*Rosters*' section on KURA is not maintained by the Ministry's IMU (Health). Thus, whilst the Medical Co-ordination unit within MDH maintains and uploads the '*Doctors Daily Duty Rosters*' worksheet on KURA on a daily basis, the '*Medical Specialities on Call Roster*' worksheet is maintained and uploaded by the Department of Medicine once a week.

Whilst reviewing the KURA portal, the NAO noted that registered users could make use of a number of services, such as requesting the creation of a physical patient file, or raising an urgent request for the retrieval of a patient's physical file from the Medical Records department.

Finally, the NAO was provided with a statistical report on the usage of KURA and noted that in 2014, the total number of hits recorded on the KURA portal amounted to 352,998. In the meantime, at the time of the IT audit, the total number of hits recorded by the end of August 2015 amounted to 262,757. Taking into consideration the average number of hits recorded in 2015, it is expected that an increase in the total number of hits to reach around 394,137.

5.5.2 MDH Website

The MDH website is accessible through the following Uniform Resource Locator (URL) **http://health.gov.mt/en/MDH/Pages/Home.aspx**, which is hosted and backed up by MITA and complies with the Government's '*Website Content and Presentation Standard*'[22].

The NAO noted that the MDH website was revamped in Q1 2015 and was officially launched in July 2015, under the MEH portal[23]. The latter is now based on Microsoft SharePoint and incorporates all the services, official bodies, resources and e-Services that fall under the responsibility of the MEH. Whilst the Office of the Parliamentary Secretary for Health owns the MEH portal, every Health entity is

[22] https://www.mita.gov.mt/en/GMICT/Pages/Websites.aspx
[23] http://health.gov.mt/en/Pages/health.aspx

responsible for updating its website content. In this regard, an ICT Application officer, within the IM&T unit, is responsible for the updating of the MDH website and liaises with the Ministry's IMU (Health) when applicable.

Whilst reviewing the MDH website in terms of usability and content management, the NAO noted that the MDH website has a number of broken links or missing information:

- when clicking on the '*Management*' tab, no information is displayed as the content is still being updated;
- under the '*Wards*' tab, a number of wards have missing links and are not updated;
- similarly, the '*Day Care*', the '*Outpatient department*', the '*Clinical services*' and the '*Support Services*' tabs have a number of missing links and are not updated; and
- the '*Search*' function within this website does not work. For instance, when searching for the '*Ophthalmic ward*', within this site (not the domain), the '*Search*' function does not return any result.

During the course of the IT audit, the NAO provided a list of the above-mentioned findings to the Ministry's IMU (Health) to address these issues with the relevant stakeholders. However, at the time of the drafting of this report, the above-mentioned findings still existed. In this regard, the NAO recommends that these shortcomings should be rectified as early as possible and that Management ensures that the website is updated and made more informative to the general public.

5.5.3 Social Media

Social media is a source of information for the benefit of the individual, and serves as a platform to collaborate, interact, and exchange knowledge with different stakeholders. As a result, over the past few years, social media sites such as Twitter and Facebook, have taken over our lives and have made us closer to other parts of the world through the social interaction among people in which they create, share or exchange information, ideas and pictures/videos in virtual communities and networks.

The NAO recognizes the fact that a number of Government departments have embraced social media and created their official Facebook page to enhance virtual communication and interaction with other Government departments, agencies and the general public.

In this regard, during the course of the IT audit, the NAO observed that MDH has an official Facebook page, which was launched in Q2 2015 and is currently being maintained by the MDH Customer Care department. The Facebook page is continuously being updated with notices and events happening at MDH. However, whilst most of the notices are written in both English and Maltese language, the NAO observed that certain notices are only written in either Maltese or English. Taking into consideration that foreign-speaking individuals might be members of this page, the MDH is of the opinion that notices should always be written in both Maltese and English language. Finally, the NAO noted that the official MDH Facebook page has 4,781 likes and has an average rating of 4.7 out of 41 reviews.

In the meantime, at the time of the drafting of this report, the NAO observed that another, unofficial MDH Facebook page exists, which has 4,071 likes and an average rating of 4.0 out of 794 public ratings. Moreover, this unofficial Facebook page, which has 30,585 visits, is mainly used by the general public, who are members of this page, and mainly upload a number of personal photos while they are recovering or visiting a relative or a friend at MDH. Furthermore, certain members of this page are even uploading certain comments, either to vent their frustration or to thank the MDH staff for their care and attention whilst receiving treatment at MDH without knowing that this is an unofficial MDH Facebook page.

In this regard, since the general public might not be aware that both an official and an unofficial MDH Facebook page exist, the NAO is of the opinion that the MDH Customer Care department should promote the official MDH Facebook page by providing links on the MDH website and ensure that these pages are continuously updated. Furthermore, the NAO is concerned on the presence of the unofficial MDH Facebook page and is of the opinion that the MDH Customer Care department should also seek advice on the presence of this page as it is misleading the general public in thinking that this is the official MDH Facebook page.

5.6 Risk Management

The process of risk management is designed to reduce or eliminate the risk of certain kind of events happening or having an impact on any organisation. It thus entails in identifying, assessing and prioritising risks of different kinds, and once the risks are identified, devising a plan to minimise or eliminate the impact of negative events.

During the course of the IT audit, the NAO observed that MDH does not have a formalised IT Business Continuity and Disaster Recovery plans at the organisational level, covering all the critical IT components within MDH. However, since most of MDH's IT systems are hosted at MITA's Data Centres, MITA has implemented a number of measures to mitigate the risks involved in the event of a disruption or total failure in the IT systems and network infrastructure within MDH. In the meantime, at the time of the IT audit, MDH still had a number of IT systems, which were hosted at the MDH Data Centre and maintained by the IM&T unit. However, as highlighted earlier on, the NAO was informed that discussions were underway between the IM&T unit and MITA on the possibility of migrating the existing IT systems and NAS devices to MITA's Data Centres.

In the meantime, the NAO noted that various MDH officials have drafted a number of Standard Operating and Downtime procedures for most of the software applications selected for the purpose of this IT audit, such as CPAS and Centricity RIS and PACS. Whilst the NAO commends the initiative in drafting these procedures, the NAO recommends that MDH should ensure that every software application should follow the same route and that these documents are continuously updated. Furthermore, every MDH user should be aware of and follow these procedures, especially whenever there is a disruption or total failure in the IT systems or network infrastructure.

The NAO is of the opinion that, notwithstanding that most of the IT systems are hosted at MITA's Data Centres and the network infrastructure is monitored and maintained by MITA, MDH should perform

a Business Impact Analysis and a Risk Assessment exercise from which a Business Continuity and Disaster Recovery plan can be drafted at the organisational level as depicted in Appendix E.

5.6.1 Business Impact Analysis

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

The Business Impact Analysis process is based upon the information that is collected from the IM&T unit and key users within MDH. The information can be collected using different approaches, such as the questionnaire approach, whereby a detailed questionnaire is circulated within the IM&T unit and to key users within MDH. Another alternative is to interview a number of key users. In the end, all the information gathered during these interviews or from the questionnaire response, is tabulated and analysed, from which a detailed Business Impact Analysis plan and strategy is drafted.

In addition, the NAO is of the opinion that MDH lists and reviews its critical and non-critical functions, and from each critical function, MDH should then determine:

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

- ***Recovery Time Objective (RTO)*** – the acceptable downtime in case of a disruption of operations. It indicates how long it will take to restore data and resume the business operations after a disaster occurs.

Once the above process is completed, MDH should then determine its recovery requirements. This will identify the business and technical requirements to recover each system or critical function in the event of an interruption, including disasters, and to provide guidance based on which detailed recovery procedure is to be adopted.

5.6.2 Risk Assessment

The NAO believes that a cost-effective BCP and DRP need to be part of a disciplined risk management approach, which should include an analysis of business processes, and the risks that these processes face. If MDH fails to identify the above-mentioned risks, it can neither plan nor manage the processes to mitigate those risks.

The NAO recommends that MDH should carry out a risk assessment to analyse the value of its assets, identify threats to those assets and assess the level of vulnerability to those threats. Fires, floods, acts of terrorism/sabotage, hardware/software failures, virus attacks, DoS attacks, cyber crimes and

internal exploits are all examples of the type of threats that are to be analysed, assigning a probability assessment value to each.

In this regard, the NAO is of the opinion that a risk analysis is implemented to define the preventive measures that will reduce the possibility of these threats occurring, and to identify countermeasures to successfully deal with these threats, if and when they develop. As a result, a well-defined risk-based classification system should determine whether a specific disruptive event requires initiating a BCP or a DRP.

5.6.3 Business Continuity Plan and Disaster Recovery Plan

The primary objective of a Business Continuity Plan (BCP) is to protect MDH in the event that all or parts of its operations and/or Information Systems are rendered unusable, and to help MDH recover from the effects of such events.

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

Whilst a BCP refers to the activities required to keep MDH operations running during a period of interruption of normal operation, a Disaster Recovery Plan (DRP) is the process of rebuilding the operations or infrastructure following a disaster.

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

As highlighted above, even though most of the IT systems are hosted at MITA's Data Centres and the network infrastructure is monitored and maintained by MITA, MDH should still draw up a formal BCP and DRP plan, designed to reduce the impact that the disruptions might inflict on MDH's operations.

Finally, when the DRP has been concluded, this should be tested regularly. Moreover, the key persons should familiarise themselves with the recovery process and the procedures to be followed in the event that the DRP is invoked. This will evaluate the effectiveness of the recovery documentation and establish whether the recovery objectives are achievable. The final result is to identify any improvements required in the Disaster Recovery strategy, infrastructure and the recovery processes established in the DRP.

Chapter 6

Management Comments

Chapter 6

Management Comments

Mater Dei Hospital's Management would like to thank the National Audit Office Officials for conducting an IT Audit at MDH. Management is committed to improve the services provided by our hospital and recognises that there is definitely room for improvement. In this regard, MDH Management is committed towards continuous service improvements and will implement any recommendations put forward by the NAO which are feasible in the operational context of MDH.

IT Management

a. NAO has noted that the reliance on one ICT Applications Officers to support the various critical software applications and recommended the allocation of additional human resources to support software applications and the filling of vacated posts in the networks team. In this regard, MDH is liaising with Ministry officials in order to replenish Human Resources in the IT Department.

b. NAO has recommended that MDH analyses the options so that patient's health information may be scanned and saved electronically in order to reduce the volume of the physical files and the storage space required. MDH is fully aware of the situation and is exploring offsite and intelligent storage solutions to cater for this. In this regard, MDH is liaising with Legal representatives and the National Archives for guidance.

c. NAO has recommended that the IT Training section offers e-Learning and m-Learning facilities. In this regard, MDH is currently liaising with the Ministry IMU in order to introduce a collaboration intranet solution throughout Health. MDH is planning to launch e-Learning material about its application to this solution.

d. NAO recommended that MDH IT Strategy is given its due importance. In this regard, MDH IT is working in collaboration with Ministry to finalise MDH Strategy to make sure that it fits with the strategy of the same Ministry.

e. NAO recommended that hard disks are wiped when they are disposed or when PCs are transferred. While MDH has already adopted this wiping application it will endeavour to ensure that method is used for both disposed of and transferred PCs.

IT Applications

a. The recommendation made by NAO about Access Dimensions has been taken onboard, MDH through Ministry Officials has requested a meeting with the Supplier in order to decommission the old server and move the application to a SHE.

b. NAO's recommendation about RIS has been taken onboard and any RIS application installations are now required to be approved by the ICT Manager.

c. NAO's recommendation about the old PAS has been taken onboard, MDH will ensure that this is carried out as soon as possible.

d. NAO's recommendation about the importance that users must update patient demographics and enhancements required is noted, an initiative to reach out to Hospital users in an effort to update and enhance patient data will be taken in the near future. Regarding the registration of deceased on Health Information Systems, while there is communication with Registry, the gap of when Health is notified needs to be minimised.

e. NAO's recommendation about evaluating the provision of elevated privileges to specific users so that modifications in booking slots may be carried, MDH noted that management of booking slots is strictly at the discretion of Clinicians, MDH is exploring the possibility to increase number of super users.

f. NAO's recommendation about enabling the Dakar audit trail functionality is noted. In this regard, a Steering Committee has been setup at Ministry level in order to review HR systems, MDH is represented on this committee, and such matters are being looked into.

g. NAO recommends that MDH's management should review its payroll business process holistically and assess the possibility of enhancing the current system is noted. MDH will be working through the steering committee to improve the payroll business process.

h. With reference to NAO's recommendation about access to medical records of children by parents or guardians through myHealth, NAO may wish to note that such access is available by means of the Patient consent scheme through GPs as per the current protocol.

i. With reference to NAO's recommendation to integrate different systems with CPAS and corporate databases, NAO may wish to note that MDH favours integration of systems and is committed towards achieving full integration, however, integration requires substantial efforts and thus it is an ongoing process.

Information Security

a. NAO's recommendation about the drafting of policy about the disposal of confidential information saved in electronic format is noted. MDH is in process of drafting such a policy for eventual approval and distribution.

b. NAO's recommendation is noted, in order to remind responsible officers of their obligations, an internal memo will be issues to heads of sections.

c. NAO's recommendation is noted, to make a regular review of user accounts. MDH is reviewing accounts on a regular basis together with MDH HR and Ministry's IMU. A process to notify System Administrators of employee movement has also been initiated and MDH with the help of Ministry's IMU intends to fine tune it to include all Ministry in this exercise.

d. As regards, to password management best practices, while NAO comments are noted, NAO may wish to note that for users to access applications, they must log through the Government Domain account that already adheres to the GMICT Password policy. Having said this, where improvements are possible MDH will make contact with the respective suppliers to improve further. MDH, together with Ministry's IMU and MITA is also looking towards implementing a Single Sign On solution so that the management of accounts and access to applications may be carried out through such solutions by means of the Government account credentials.

IT Operations

a. NAO recommendation about the issuing a memo so that users are guided the proper channels when logging calls for assistance related to IT systems is noted. While users are provided guidance on which escalation process to use, MDH will issue such a memo accordingly.

b. As per NAO's recommendation about guidelines for the backup and storage of offline emails, internal memos have been issued. In this regard, MDH is planning to make available such a guideline on the new intranet through IT Trainers.

c. Regarding the recommendation made by NAO about broken links, NAO may wish to note that such links were a result of old links due to the migration that was carried out from the old website to the current new website. In this regard, NAO may wish to note that all broken links reported were rectified. MDH is also committed in making its website more informative to the general public.

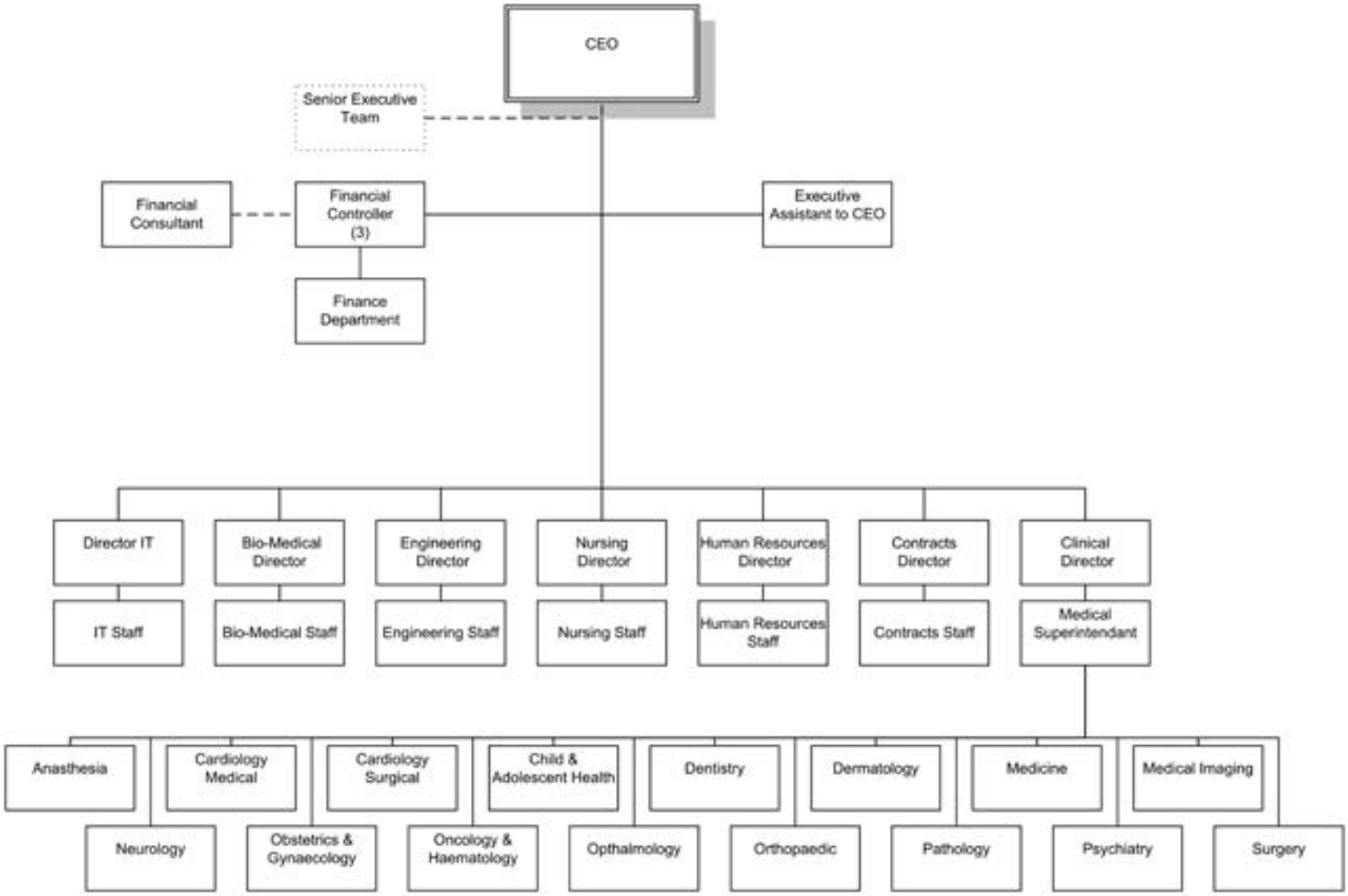
d. Regarding the recommendation made about the MDH facebook, NAO may wish to note that MDH is liaising with Ministry IMU so that all official social media pages approved by Health authorities are displayed in a specific page on Health's website, thus, the public will be made aware about which are official social media pages used by MDH.

e. The recommendation to conduct a Business Impact Analysis and a Risk Assessment exercise from which a Business Continuity and Disaster Recovery plan can be drafted at the organisational level is taken onboard.

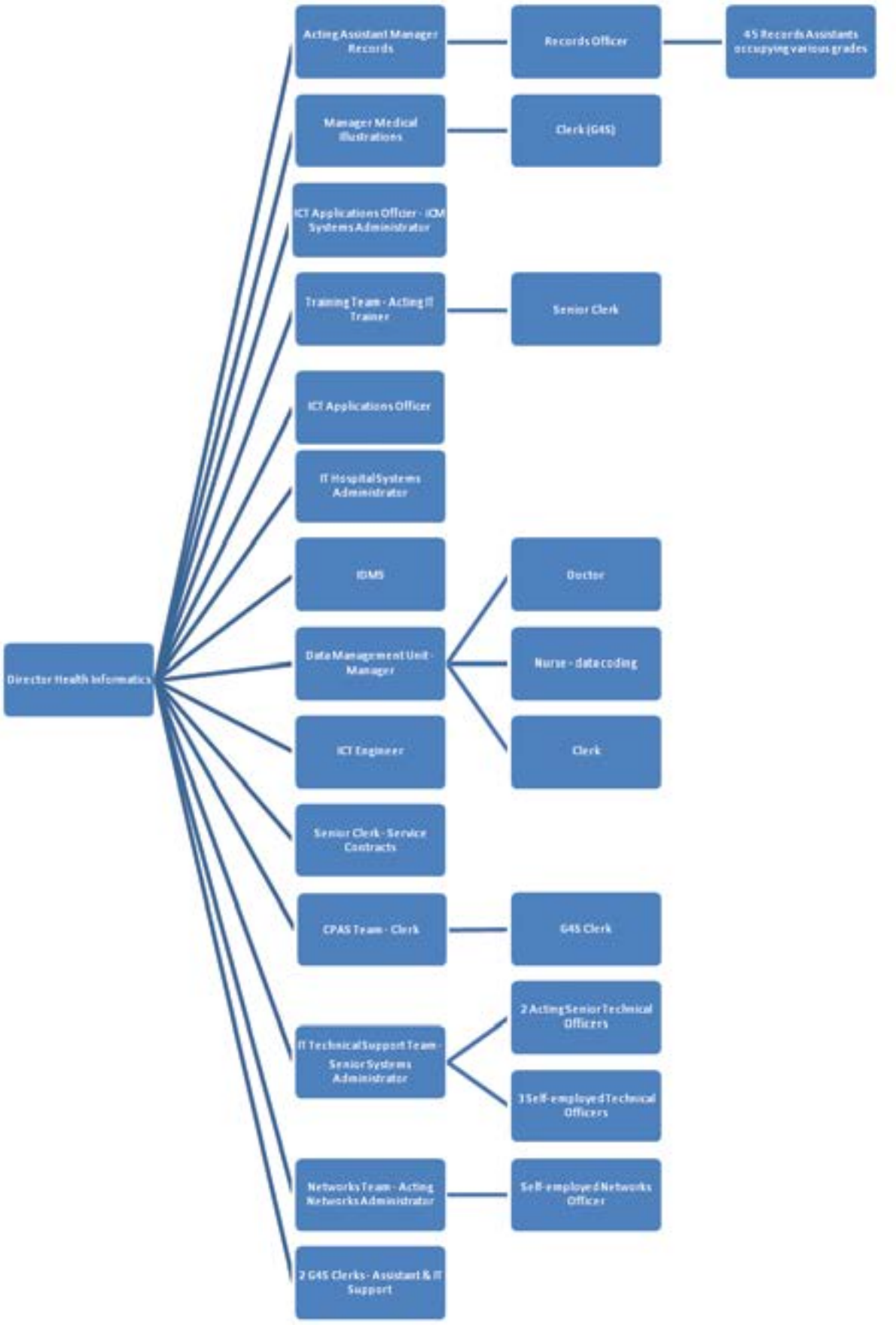
f. Regarding NAO's recommendation for awareness to MDH user about procedures to be followed in the event of disruption or failure of IT services, MDH keeps the respective heads and critical users informed. Moreover all users are informed through an internal memo together with instructions on what services will be impacted and type of downtime procedures to be followed. However, NAO's comments are noted and a review of downtime procedures will be taken.

Appendices

Appendix A – Mater Dei Hospital Organisational Chart



Appendix B – Information Management and Technology Unit Organisational Chart



Appendix C – COBIT Controls

COBIT 4.1 defines IT activities in a generic process model within four domains[24]. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate as depicted in Figure 4. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

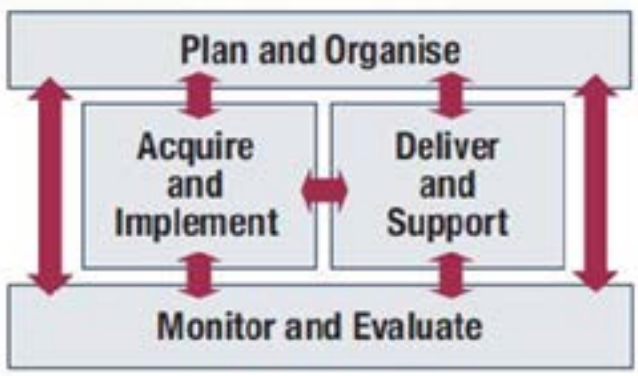


Figure 4 - COBIT Controls

Plan and Organise Domain

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

Define a Strategic IT Plan

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

Assess and Manage IT Risks

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

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

Acquire and Implement Domain

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

Manage Changes

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

Install and Accredit Solutions and Changes

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

Deliver and Support Domain

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

Define and Manage Service Levels

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

Manage Third party Services

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

Ensure Continuous Service

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

Ensure Systems Security

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

Manage the Physical Environment

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

Manage Operations

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

Monitor and Evaluate Domain

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

Provide IT Governance

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

Appendix D – Restrictions on use of e-mail and Internet Services

Restrictions on use of e-mail services

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

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

Restrictions on use of Internet services

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

- Create, willingly download, view, store, copy or transmit pornography and any other activities that are illegal, discreditable, offensive, and discriminatory or prohibited by law.
- Conduct or participate in crimes of any sort, example computer hacking, theft of proprietary data, etc.

In particular, authorised users are to refrain from seeking to impair any Internet content filtering facilities.

Appendix E – Business Continuity and Disaster Recovery Plans

A BCP should:

- Be consistent with the MDH's overall mission, strategic goals and objectives.
- Be documented and written in simple language and understandable to all.
- Provide management with an understanding of the adverse effects on MDH, resulting from normal systems or service disruption and the total effort required to develop and maintain an effective BCP.
- Identify the information assets related to core business processes.
- Assess each business process to determine its criticality.
- Validate the RPO and the RTO for various systems and their conformance to MDH's objectives.
- Identify methods to maintain the confidentiality and integrity of data.
- Ensure that an appropriate control environment (such as segregation of duties and control access to data and media) is in place.
- Ensure that data is regularly backed up on storage media.
- Ensure that appropriate backup rotation practice is in place and backups are retrievable.
- Ensure that storage media are kept offsite and kept securely in a backup safe.
- Identify the conditions that will activate the contingency plan.
- Identify which resources will be available in a contingency stage and the order in which they will be recovered.
- Identify the key persons responsible for each function in the plan.
- Identify the methods of communication among the key stakeholders.
- Implement a process for periodic review of the BCP's continuing suitability as well as timely updating of the document, specifically when there are changes in technology and processes, legal or business requirements.
- Develop a comprehensive BCP test approach that includes management, operational and technical testing.

- Implement a process of Change Management and appropriate version controls to facilitate maintainability.

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

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

A DRP should contain the following information:

- A statement detailing the scope and capability of the DRP, exactly when should this plan be used and what is the impact on MDH.

- A description of the key roles and responsibilities so that anyone assigned to a particular role in the recovery team understands what is required of them.

- A summary of the critical services, their recovery objectives and recovery priorities.

- Third party contact details, particularly those that may be required to assist in the recovery of resources or services that are being maintained within MDH.

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

RECENT AUDIT REPORTS ISSUED BY THE NAO

NAO Audit Reports

May 2015	Audit of Gozo Channel Company Limited: Public Service Obligation Bid Feasibility and Operational Considerations
June 2015	Performance Audit: Class Size in State Primary Schools
July 2015	A Comparison of Crude Oil Prices and Electricity Tariff Band Structures
July 2015	Performance Audit: Tackling Domestic Violence
July 2015	Information Technology Audit: Housing Authority
October 2015	An Investigation of matters relating to the Emphyteutical Contract between Government and the General Workers Union
November 2015	An Investigation into the Issuance of Encroachment Permits between December 2012 and March 2013
December 2015	Annual Audit Report of the Auditor General - Public Accounts 2014
December 2015	Annual Audit Report of the Auditor General - Local Government 2014
January 2016	An Investigation of Government's Expropriation of Two One-Fourth Undivided Shares of the Property at 36 Old Mint Street, Valletta
February 2016	Performance Audit: Agreements between Government and Conservatorio Vincenzo Bugeja on Jeanne Antide and Fejda Homes
February 2016	Performance Audit: Service Agreements between Government and INSPIRE Foundation
April 2016	Performance Audit: An Analysis on OHSA's Operations A Case Study on the Construction Industry

NAO Work and Activities Report

March 2016	Work and Activities of the National Audit Office 2015