NAO
National Audit Office
MALTA

Information Technology Audit

Armed Forces of Malta

Report by the Auditor General

February 2014

Information Technology Audit

Armed Forces of Malta

Table of Contents

List of Tables

List of Figures

List of Abbreviations

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

AD	Active Directory
ADSL	Asymmetric Digital Subscriber Line
AFG	Army Form General
AFM	Armed Forces of Malta
AIS	Automatic Identification System
ATCC	Aid to the Civil Community
ATCP	Aid to the Civil Power
BCP	Business Continuity Plan
C3I	Command, Control, Communications and Information Company
CASEVAC	Casualty Evacuations
CCTV	Closed Circuit Television
CDRT	Centre for Development, Research and Training
CIMU	Central Information Management Unit
CIO	Chief Information Officer
CIS	Communications Information Systems
CMO	Crisis Management Operations
COBIT	Control Objectives for Information and related Technology
CQMS	Company Quarter Master Sergeant
CSDP	Common Security and Defence Policy
DAS	Departmental Accounting System
DHCP	Dynamic Host Configuration Protocol
DMS	Document Management System
DoS	Denial of Service
DRP	Disaster Recovery Plan
DSC	Digital Selective Calling
EBF	European Border Funds
E-mail	Electronic Mail
EOD	Explosive Ordinance Disposal
eRFS	Electronic Request for Service
ETO	EUROSUR Technical Office
EU	European Union
EUROSUR	European Border Surveillance System
EVRF	Emergency Volunteer Reserve Force
FEAR	Force Element at Readiness
FMS	Fleet Management System
GMDSS	Global Maritime Distress Safety System
GMICT	Government of Malta Information and Communication Technology

HD	High Definition
HRMIS	Human Resources Management Information System
ICS	Integrated Communications System
ICT	Information and Communications Technology
IEDD	Improvised Explosive Device Disposal
IMU	Information Management Unit
IT	Information Technology
ITSM	Information Technology Service Management
kHz	Kilo Hertz
LAN	Local Area Network
LPO	Local Purchase Order
MAGNET	Malta Government Network
Mbps	Megabits per second
MCL	Microwave Carrier Link
MCAST	Malta College of Arts, Science and Technology
MEDEVAC	Medical Evacuation
MITA	Malta Information Technology Agency
MITC	Ministry for Infrastructure, Transport and Communications
MF	Medium Frequency
NAO	National Audit Office
NATO	North Atlantic Treaty Organisation
NAVTEX	Navigational Telex
NCA	National Competent Authority
NCC	National Co-ordination Centre
OA	Office Automation
OPM	Office of the Prime Minister
OS	Operating System
OSCE	Organisation for the Security and Co-operation in Europe
PI	Public Information
PC	Personal Computer
PfP	Partnership for Peace
P&C	Progress and Report
QM	Quarter Master
RAID	Redundant Array of Independent Disks
RCC	Rescue Co-ordination Centre
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SQL	Structured Query Language
SQM	Staff Quarter Master
UPS	Uninterrupted Power Supply

VHF	Very High Frequency
VIP	Very Important Person
VPN	Virtual Private Network
VTMIS	Vehicle Traffic Management Information System
VTS	Vessel Traffic System
WAN	Wide Area Network
WSUS	Windows Server Update Services

Executive Summary

Executive Summary

Background

The National Audit Office (NAO) carried out an Information Technology (IT) audit within the Armed Forces of Malta (AFM) between June and October 2013. This audit sought to examine AFM's IT operations, AFM's IT investments and their alignment with the AFM strategic objectives.

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

Key Findings and Recommendations

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

a. The AFM Microwave Carrier Link (MCL) network, which links Malta's radars and sensor stations with the Operations Centre in Luqa Barracks, required immediate upgrade and/or replacement. The data communication networks, linking the respective AFM units, were inefficient and slow due to insufficient bandwidth.

b. In 2011, the Headquarters AFM Communications Information System (CIS) Section was tasked to assume the lead and form a strategic partnership with the Information Management Unit (IMU) within the Office of the Prime Minister (OPM), to drive the required IT matters and align IT as a support enabler for military and security operations.

c. Following the recommendations and consultations held between the previous AFM CIS representative, MITA and the IMU OPM in 2010 and early 2011, the Headquarters AFM CIS Section opted to follow the advice to move towards a "Federated" CIS architecture.

d. In November 2011, a paper entitled *"Outlining the Armed Forces of Malta Communications and Information Systems Concept towards a Federated Environment"* was published. It identified two infrastructural elements that were deemed essential by the AFM to adopt a Federated model.

e. The NAO noted that in 2013, the AFM budgeted for two core infrastructural projects that would enable the AFM to assume the above mentioned Federated model. These projects included a new Data Centre to consolidate all the AFM CIS services, applications, networking and communications infrastructure and to upgrade the existing AFM Wide Area Network (WAN) with the required bandwidth to support the overall AFM operations and administration.

f. The NAO was informed that the AFM MCL network had reached technological obsolescence and cannot be upgraded any further. However, the AFM IT Strategy highlights the importance of having an autonomous operational WAN, which would have sufficient bandwidth to eventually support the AFM operations and administration. In this regard, the NAO recommends that the Headquarters AFM CIS Section should ensure that this plan is followed through and implemented.

g. The NAO recommends that even though it was observed that the AFM Procurement and Logistics Branch maintain the overall IT inventory in a very efficient and structural way, the AFM should refine their current inventory process and invest in an electronic IT inventory application whereby all the hardware and software assets are stored centrally.

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

a. The NAO was informed that the European Border Surveillance System (EUROSUR) system, contrary to the recommended synchronous fibre-optic connection, is running on an ADSL internet connection with a local communications service provider. Moreover, to-date the AFM does not have a redundant internet connection to this node.

b. In 2013, the European Union (EU) Council adopted a regulation establishing the EUROSUR system as one of the key tools at its disposal to prevent any tragedies at sea. Since the AFM is the designated national authority on integrated maritime surveillance, the NAO recommends that the AFM monitors the outcome of this regulation and ensures that the AFM has enough resources that are familiar with the use and the daily monitoring of the EUROSUR system.

c. The NAO observed that the Integrated Communications (Radio over IP) System (ICS) is not covered by a Service Level Agreement (SLA). In the absence of a formal SLA, the service levels are slow, since different modules of the ICS were assembled from hardware provided by different

foreign communication suppliers. The NAO acknowledges the effort being made by the AFM CIS Section to negotiate an SLA at this point. On the other hand, this should have been negotiated during the ICS commissioning stage.

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

a. In the absence of an official Data Retention and Storage Policy, the NAO recommends that an internal policy is formalised and distributed to all AFM officials concerned.

b. Overall, the NAO commends the number of internal policies and operating procedures that were issued by the AFM CIS Section. The NAO recommends that these should be continuously updated and ongoing.

c. The NAO is pleased to note that the AFM CIS Section developed an in-house database to cater for the management of all the user accounts in use across the AFM. This database is continuously being updated to ensure that the AFM CIS Section is in control of the management of all user accounts.

d. The NAO recommends that Information Security Awareness guidelines should be ongoing whereby AFM officials are provided regular updates to foster security awareness and compliance with security policies and procedures.

Chapter 5 of this report delved into the management and controls of IT operations to maintain data integrity and to ensure that the IT setup can successfully implement an IT disaster recovery process should the need arise.

a. The NAO noted that even though the AFM Data and Communication Rooms do not enjoy the standard facilities, which modern Data Centres are equipped with, the AFM IT Strategy envisages that a new Data Centre will consolidate all the AFM CIS services, applications, networking and communications infrastructure.

b. The NAO observed that whilst all the incidents related to third party suppliers are kept in a file, the IT Section of the CIS Company 4th Regiment, which runs all day-to-day matters concerning IT operations and support, does not keep track of any incoming internal IT service requests. Thus, the NAO recommends that all the incidents be recorded electronically in a call logging system or in a simple centralised spreadsheet.

c. With its limited resources, the AFM PI Cell goes to great lengths to update all the AFM online platforms on a 24/7 basis to serve as an information hub to the journalists and to the public.

d. During the course of this IT Audit, the NAO observed that the AFM does not have formalised IT Business Continuity and Disaster Recovery plans covering all the critical IT components within

the AFM. However, a number of initiatives were taken by the Headquarters AFM CIS Section to mitigate the risks involved in the event of a disruption or total failure in the IT systems within the AFM.

e. The NAO recommends that the AFM carries out a Business Impact Analysis to reveal the business and operational impacts stemming from IT related incidents or events. The AFM will then list and review its critical and non-critical functions. After going through this process, the AFM would then determine a recovery strategy.

f. The NAO recommends that the AFM should carry out a risk assessment to analyse critical assets, identify threats to those assets and assess the level of vulnerability.

The final chapter of this report lists the Management comments submitted by the AFM.

Chapter 1

Introduction

Chapter 1

Introduction

The AFM is Malta's national defence and security organisation tasked with the primary function of safeguarding national sovereignty and interest, both in peacetime and in crisis. The AFM is thus a major and a key component of the Island's national security architecture.

The AFM performs two main defence roles designated as 'primary' and 'secondary' defence roles. The 'primary' role ensures that the AFM develops and maintains appropriate military capabilities in the defence of the state. As a security and a defence organisation, the AFM, as the sole military instrument of national power, needs to be capable of deploying a modern, interoperable sustainable force that can deliver flexible military capabilities in critical situations to ensure the security and integrity of the Maltese Islands. In this regard, the 'primary' defence roles are to:

- Maintain territorial integrity (particularly at the Malta International Airport and other sensitive locations);
- Maintain integrity of Maltese waters (physical and electronic surveillance against smuggling, illegal trafficking of immigrants and other illicit activities at sea by conducting Maritime Law Enforcement);
- Contribute towards international peace and stability by participating in overseas crisis management operations;
- Provide for the surveillance of the Maltese Airspace;
- Provide Search and Rescue services over Maltese territorial waters and the Search and Rescue region; and
- Provide Explosive Ordinance Disposal (EOD) and Improvised Explosive Device Disposal (IEDD) cover.

The 'secondary' role of the AFM relates to the social facet of security. It entails providing military support to the Civil Government in what is referred to as the Aid to the Civil Power (ATCP) and Aid to the Civil Community (ATCC). Thus, the 'secondary' defence roles are to provide:

- Civil emergency protection support;
- Military aid to the Police and Security service; and
- State Ceremonial and other Public Support duties.

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

1.1 Background

The 'Malta Armed Forces Act' was passed through Parliament in August 1970. It enables the Head of State to raise, maintain and regulate an armed force. This Act also empowers the President of Malta, as the Head of State, to delegate the command and authority vested in him/her to the democratically elected Government, exercisable by the Minister responsible for the AFM, and answerable to Parliament.

The AFM was formed upon Malta becoming a Republic in 1974, when 1st Regiment Royal Malta Artillery was renamed as 1st Regiment AFM. This initially continued the artillery role, with 2nd Regiment formed as Engineers unit. In 1980, 1st Regiment became a mixed unit, with infantry, aircraft and maritime responsibilities, the artillery aircraft element being transferred to 2nd Regiment. In 1992, there was a major re-organisation, which led to the formation of the 3rd Regiment that remains predominantly reflected in its structure till this very day.

1.2 Organisation Structure

The overall command of the AFM is exercised by the Headquarters AFM that is located at Luqa Barracks. The Headquarters AFM operates at both the military strategic level as well as the operational level. All the AFM officials who are currently working at the Force Headquarters previously served in land, air or maritime components of the force.

At the time of this IT Audit, the Headquarters AFM was composed of a number of Branches and Sections as outlined in Appendix A. These included:

- **Personnel and Administration Branch** dealing with personnel management, manpower administration, welfare/chaplaincy, recruitment, promotions, public information, state ceremonial, civil-military co-operation and provost matters;

- **International Affairs Branch** responsible for international affairs, bi-lateral and multi-lateral affairs to include EU Common Security and Defence Policy (CSDP) matters, Organisation for the Security and Co-operation in Europe (OSCE) matters, 5 Plus 5 Defence Initiative matters, North Atlantic Treaty Organisation (NATO) Partnership for Peace (PfP) matters, military to military relations and supporting Maltese participation in overseas crisis management operations;

- **Operations, Plans and Intelligence Branch** is responsible for the co-ordination of military intelligence, land, air and maritime operations;

- **Procurement and Logistics Branch** is responsible for major procurement projects, integrated logistics and combat service support. This Branch is also responsible for health and safety, contracting works and the maintenance of the defence estate and engineering;

- **Capabilities and Training Branch** is responsible for the co-ordination of the Force's local and overseas training and education programs. This includes exercises planning and execution;

- **CIS Section** is responsible for the strategic and operational planning of the Force's CIS resources. It oversees the co-ordination, development and review of the policies and procedures for the management and use of Communications and Information Systems, including computing, telecommunications and associate resources;

- **Legal Advice Section** provides legal assistance and advice on a wide variety of military law as well as civil, administrative, operational and criminal law;

- **Financial Management Section** is responsible for the administration of the AFM Finance and Pay Offices. This section also provides advice on all matters related to public finance issues and applicable regulations. Furthermore, this section assists in the drawing up of AFM's annual budget requirements and helps exercise control over the capital and recurrent expenditure of the Force;

- **Medical Section** provides medical support to the Force including the medical supervision serving personnel for national operations and overseas deployment. This section also provides medical support when required during search and rescue and medical evacuation operations. It also provides specialist medical and fitness support to military divers, pilots and air crew.

By the time the NAO concluded the IT Audit report and held the final exit meeting, in October 2013 the AFM carried out a re-organisation of the Headquarters setup. As a result of this re-organisation and with the intent to empower the CIS function with logistical support for local and EU Projects (such as the building of a new Data Centre and the upgrading of the MCL Network), the CIS Section was integrated with the AFM Procurement and Logistics Branch, headed by Colonel Procurement and Logistics. The appointment of Staff Officer II CIS, holding the rank of Major, was established to manage the CIS strategy under the supervision of Colonel Procurement and Logistics. This move was complimented with a decision by the AFM to allocate a specific budget line for CIS usage.

In view of this organisational change, the NAO recommends that the AFM takes steps to ensure that the risks identified in this report are addressed by the team responsible for the related IT process or system and the related recommendations are implemented by allocating the required resources.

Apart from the Force Headquarters, the AFM consists of five separate units – three land units, an air wing and a maritime squadron as depicted in Appendix B. The AFM also have a Reserve and an Emergency Volunteer Reserve Force (EVRF).

- **1st Regiment AFM** – The 1st Regiment AFM is the AFM's Infantry Battalion and is based at Lyster Barracks in Ħal Far. The 1st Regiment is organised into a Headquarters Company, three Infantry Companies (including a Special Duties Company) and an Air Defence and Fire Support Company. It is the AFM's main land manoeuvre unit with the aim to:

  - Secure locations of strategic and national interest;

  - Maintain Force Elements at Readiness (FEAR) to deploy on Crisis Management Operations (CMO); and

  - Be prepared to support civil authorities in exceptional circumstances or in times of national distress.

- **3rd Regiment AFM** – The 3rd Regiment AFM is a combat support regiment whose role is to contribute support to AFM units by deploying well-trained and motivated soldiers to provide adequate service support.

  An integral part of this unit is field-engineering capability, which apart from its normal peace time support backup, also performs engineer battlefield functions for the infantry units focusing on mobility, counter mobility and survivability.

  The 3rd Regiment AFM operates from Safi Barracks and is made-up of the following units:

  - Headquarters Squadron;

  - Electrical and Mechanical Engineering Squadron;

  - Combat Engineer Squadron; and

  - Ammunition and Explosives, Storage and Disposal Squadron.

- **4th Regiment AFM** – The 4th Regiment AFM is the combat support role and provides service support to all AFM units in peace time and in times of crisis. The 4th Regiment AFM is co-located with the Headquarters AFM and the AFM Operations Centre at Luqa Barracks. The

AFM Operations Centre is the Force's Command and Control hub and doubles up as the Maltese Rescue Co-ordination Centre (RCC) co-ordinating search and rescue on land, air and sea. The 4th Regiment is made up of the following Sub-Units:

- Headquarters Company;
- AFM Band;
- CIS Company;
- Catering Company;
- Revenue Security Corps; and
- AFM Training School.

- **Maritime Squadron AFM** – The Maritime Squadron AFM provides the maritime element of the AFM and operates from Hay Wharf Quay in Pietà. The G Command, which forms part of the AFM Maritime Squadron, is based in Qortin Gozo. It consists of a land and sea element, which are necessary to cater for an immediate and swift response on the island of Gozo.

  The Maritime Squadron has a general responsibility to meet defence and contingent requirements such as maritime surveillance, maritime law enforcement. It is also responsible to execute search and rescue operations at sea, Medical Evacuation (MEDEVAC) and Casualty Evacuations (CASEVAC). Other sundry tasks include reconnaissance operations, Very Important Person (VIP) conveyances, and security escort duties at sea.

  The Maritime Squadron is made up of five different commands namely:

  - Headquarters Command;
  - Offshore Command;
  - Inshore Command;
  - G Command; and
  - Support Command.

- **Air Wing AFM** – The Air Wing AFM is located at Luqa Airport and is the aerial component of the Force. The Air Wing AFM lends itself to all deployments of air assets in various roles and missions in order to maintain the territorial integrity of the Maltese Islands. The Air Wing AFM discharges a mix of functions in providing:

  - Maritime Surveillance;
  - Search and Rescue on land and sea;
  - MEDEVAC and CASEVAC;
  - VIP and military conveyances;
  - Reconnaissance including aerial photography and filming;
  - Security escort and limited fire support; and
  - Transportation of troops.

- **EVRF AFM** – The EVRF are currently integrated into the Air Defence and Fire Support Company within the 1st Regiment AFM, where they are trained to the same level of proficiency as their regular counterparts. In an emergency, the EVRF soldiers will, amongst other duties, be expected to perform the following tasks:

  - Civil emergency duties, in support for the civil administration in the event of disasters;
  - Key point security guarding duties in an emergency;
  - Tactical infantry patrolling, surveillance and providing fire support.

At the time of this IT Audit, the AFM had a staff compliment of 1,517 full-time male and 60 full-time female employees as depicted in Table 1 below. To-date, the AFM does not have any employees working on teleworking or reduced hours.

AFM Units	Male	Female
Headquarters AFM	105	13
1st Regiment AFM	459	32
3rd Regiment AFM	263	2
4th Regiment AFM	267	8
Air Wing AFM	100	2
Maritime Squadron AFM	305	Nil
EVRF	18	3
Total	**1,517**	**60**

Table 1 – Human Resources at AFM

1.3 Legislation

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

- The Malta Armed Forces Act, Cap 220 of the Laws of Malta;
- Designation, Command and Establishment of the Armed Forces of Malta Order, S.L. 220.02;
- Assignment of Powers to Armed Forces of Malta Order, S.L. 220.06;
- Territorial Waters and Contiguous Zone Act, Cap 226;
- Military Equipment (Export Control) Regulations, S.L. 365.13;
- Airports and Civil Aviation (Security) Act, Cap 405;
- Fisheries and Conservation and Management Act, Cap 425;
- Malta-USA Ship-Boarding Agreements (Ratification) Act, Cap 493;
- Criminal Code, Cap 9;
- Customs Ordinance, Cap 37;
- General Authorisations (Radio Communications Apparatus) Regulation, S.L. 49.09;
- Simplifying terms and conditions of transfers of defence-related products regulations, S.L. 117.32

1.4 ICT within the AFM

Considering that, the AFM is Malta's national defence and security organisation, the AFM is increasingly dependent on Information and Communications Technology (ICT) to be able to carry out its operations and to process, store and maintain the necessary information.

Apart from the Office Automation (OA) software applications, the AFM make use of a number of IT application systems, which include:

- **AFM Human Resources Management Information System (HRMIS)** – It is a multi-user Management Information System, which covers payroll, AFM personnel information and medical data;
- **Coastal Radio Station** – The Malta Coast Radio Station monitors shipping, radio distress frequencies and relays ship-to-ship and ship-to-land communications;

- **Departmental Accounting System (DAS)** – It is the main accounting system in use to record and control expenditure and revenue across all Government departments;

- **Document Management System (DMS)** – The DMS facilitates the digitisation of documents and automates the administrative business processes of the AFM (filing, registry of documents, correspondence etc.) for ease of access;

- **EUROSUR** – The EUROSUR is an EU system intended to setup a permanent connection among EU member states and Frontex, to provide a fully extensible information sharing system for both non-classified as well as classified information related to border control operations;

- **Fleet Management System (FMS)** – It is used to issue and keep track of fuel chits for AFM vehicles;

- **ICS** - The system functionality enables the networking of radios and other communications equipment into a single operational network. It supports voice and data communications including the receipt and transmission of documents, images and video. This system can thus be considered a critical enabler supporting both national and international operations;

- **Vessel Traffic Management Information System (VTMIS)** – The Malta Coastal VTMIS provides 24/7 maritime surveillance and monitoring. The system supports the AFM in their search and rescue operations and border management control.

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

- AFM HRMIS;

- Coastal Radio Station;

- EUROSUR;

- ICS; and

- VTMIS.

The NAO also reviewed the management and maintenance of the AFM Website, the AFM Facebook page, the AFM YouTube Channel, the AFM Intranet and the ICT Infrastructure, which consists of:

- **Servers** – The AFM has three physical servers running on Microsoft Operating System (OS) platform that includes:

    - An Active Directory (AD) Domain Controller;

    - A centralised backup server to provide a near-continuous data protection and data recovery in a Microsoft Windows environment;

- A dedicated server hosting a number of virtual environments, which include amongst others a Dynamic Host Configuration Protocol (DHCP) server, a Structured Query Language (SQL) Server, a Mirrored AD Domain Controller, a File Sharing Server and an Intranet Server.

- **Personal Computers (PCs) and laptops** – The PCs and Laptops were acquired through the Government leasing agreement. At the time of this IT Audit, the AFM utilises 264 PCs and 64 Laptops;

- **Network** – The Headquarters AFM, the Operations Centre and the 4th Regiment AFM which are co-located at Luqa Barracks are connected to the Malta Government Network (MAGNET) through a fibre-optic connection. On the other hand, all the remaining AFM units, namely the 1st Regiment (Ħal Far), 3rd Regiment (Safi), Maritime Squadron (Pietà), the Air Wing (Luqa Airport), Gozo Command (Qortin, Gozo), Air Defence and Fire Support Company (Luqa Airport) are individually connected to the MAGNET through an Asynchronous Digital Subscriber Lines (ADSL) bridge connection. Whilst the WAN infrastructure is monitored and maintained by MITA, the Local Area Network (LAN) infrastructure falls under the responsibility of the CIS Company within the AFM;

- **AFM MCL Network** – It is the core operational network infrastructure and communications backbone for the VTMIS, Global Maritime Distress Safety Signal (GMDSS) Coastal Radio Station and the ICS;

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

- **OA software applications** – Microsoft software licences are acquired through MITA under the Government Enterprise Agreement. Other software licences are procured through their local representative.

1.5 Audit Scope and Objectives

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

The IT audit was divided into three different stages:

- Initially, a pre-audit questionnaire was sent to the Senior CIS Officer responsible for the Headquarters AFM CIS Section, to gather the necessary information on the audit site prior to undertaking an on-site audit. The aim of the questionnaire was to familiarise the audit team with the AFM and its IT setup prior to the audit visit;

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

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

In a nutshell, the objective of this report was to:

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

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

- List all the findings and identify any potential risks;

- List all the recommendation to mitigate those risks.

1.6 Audit Methodology

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

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

1.7 Structure of the Report

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

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

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

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

- Chapter 5 analyses whether the AFM are managing and controlling their IT operations in the most effective way. Furthermore, it addresses whether the AFM are confident with any business continuity or disaster recovery plans in the event of a service disruption;

- Chapter 6 lists all the management comments.

1.8 Acknowledgement

The NAO would like to express its thanks and appreciation to all the officials within the AFM, who were involved in this audit in particular the Commander AFM, CIS Staff Officers and the CIS Section personnel, for their time, patience and assistance.

Chapter 2

IT Management

Chapter 2

IT Management

2.1 Background

The AFM Headquarters is made up of five Branches and four Sections, as depicted in the AFM Organisational Chart found in Appendix A, namely:

- Personnel and Administration Branch;
- Operations, Plan and Intelligence Branch;
- International Affairs Branch;
- Capabilities and Training Branch;
- Procurement and Logistics Branch;
- Legal Advice Section;
- Financial Management Section;
- Medical Section; and
- CIS Section.

The raison d'être of the AFM as a military organisation is to develop and maintain operational capabilities. The CIS function serves as an essential combat support enabler for military operations to provide commanders at all levels with the means to exercise command and control through secure communications, whilst also supporting various AFM elements through the design and implementation of Information Systems structures. Moreover, the CIS function within the Headquarters AFM, ensures that the IT Strategy is kept aligned with the overall AFM Strategy.

In August 2011, following an update of the AFM Headquarters Organisational Establishment, the AFM CIS Section was formally established. Prior to the establishment of the CIS Section at the Headquarters AFM, the CIS Section was an autonomous section under the Camp Commandant Regiment, which included the Command, Control, Communications and Information Company (C3I) within the 4th Regiment AFM (now superseded by the CIS Company 4th Regiment AFM).

The previous CIS Sections were only responsible for the technical, operational and user support elements. The AFM IT Strategy fell under the responsibility of the AFM Personnel and Administration Branch, however, it was delegated to the IMU OPM. The policies adapted by the AFM were those published by MITA for Government Departments, namely the Government of Malta Information and Communication Technology (GMICT) policies, directives, procedures and standards. During this time, the administration of the Force's Server Infrastructure was remotely managed by MITA, and the AFM was completely dependent on MITA for the provision of this service.

In 2010, the AFM's file sharing servers had reached their maximum capacity, the backup operations were failing and the user accounts residing on the Microsoft Windows NT User Manager needed to be migrated to a new Windows Server version, since the Microsoft Windows NT had reached its end-of-life support from Microsoft. In this regard, the IMU OPM provided the required funding to replace the existing servers, which included an SLA. Furthermore, the AFM MCL network, which links Malta's radars and sensor stations with the Operations Centre in Luqa Barracks, required immediate upgrade and/or replacement. The data communication networks, linking the respective AFM units, were inefficient and slow due to insufficient bandwidth. Moreover, the AFM Headquarters and the Operations Centre at Luqa Barracks had a laser wireless connection, rather than a direct fibre-optic connection with MITA. Internally, the AFM had already invested in a number of fibre-optic connections to enhance communications from one building to another to access the MAGNET. The AFM lacked basic hosting facilities for its system servers, a new Internet website was being commissioned and there was no presence of Social media. Moreover, the Air Wing AFM required an upgrade to the existing network infrastructure due to the building of a new hanger.

In January 2011, the AFM, after consulting with MITA and the IMU OPM, identified two possible strategies suitable for the AFM, either to consolidate the services with MITA or to move towards a federated approach.

In this regard, the Headquarters AFM CIS Section was tasked to assume the lead and form a strategic partnership with the IMU OPM to drive the required IT matters, and align IT as a support enabler for military and security operations. The CIS Section took over the responsibility for the co-ordination, development and review of governance policies and procedures for management and the use of all the communications and Information Systems resources within the AFM. To date, the CIS function within the Headquarters AFM leads the strategic and operational policy planning of the AFM. The CIS Governance also falls under the remit of the Headquarters AFM CIS Section (together with the then IMU OPM), whereby the IT Governance policy directions and operating procedures were officially published and distributed across the AFM, based upon the GMICT policies. The Headquarters AFM CIS Section, together with the IMU OPM, also promoted and monitored the strategic relationships between the AFM and external entities, including Government departments, vendors and the review

of maintenance contracts. It also approved, prioritized and controlled projects related to the selection, acquisition, development and installation of major Information Systems and networks. On the other hand, the IMU OPM was responsible for the AFM's IT Budget.

Through the above initiatives, the AFM have met their objectives, providing value to the AFM Communications and Information Systems resources as joint operational enablers for military and security operations. The Headquarters AFM established a good working relationship with MITA at the strategic and organisational level to assist the auditee to develop and sustain this capability.

2.1.1 CIS Company 4th Regiment

The CIS Company 4th Regiment is the designated service provider of CIS Services to the Force and its mandate is to provide effective communications, navigation, radar and information system to the Force, in support of operations and administration. The CIS Company 4th Regiment also provides individual volunteer augmentees to participate in oversees humanitarian and crisis management operations, provides support at short notice to internal security operations, provides military aid to the civil power following a request and also participates in ceremonial duties.

The CIS Company 4th Regiment is managed by a Captain holding the appointment of Officer Commanding CIS Company and reports to the Commanding Officer 4th Regiment AFM. The NAO was informed that the CIS Company 4th Regiment is not a subordinate to the Headquarters AFM CIS Section but follows those policies and standards that are issued from the AFM Headquarters from time to time.

To date, the established military strength (the different military ranks and human resources capabilities within the AFM) of the CIS Company 4th Regiment amounts to 76 officials. However, to date, the actual military strength amounts to 70 officials and is composed of a number of sections as depicted in Table 2.

Section	Function	Established Military Strength Officers	Established Military Strength Men	Total Established Military Strength	Actual Military Strength
Company Headquarters	Headquarters of the CIS Company	2	4	6	7
Signals Platoon	Manage and operate the Operations Centre AFM		40	40	34
Riggers Section	Maintenance and upkeep of the communication masts		7	7	6
IT Section	Support and provision of IT services		7	7	8
Technical Support Section	Telephony and network support, and infrastructural works		5	5	5
Outpost Section Madliena	Coastal Lookouts		4	4	4
Outpost Section DIngli			4	4	3
Outpost Section Delimara			3	3	3
Sub Total				**76**	**70**

Table 2 – CIS Company 4th Regiment

The CIS Company 4th Regiment is organised into the Company Headquarters, the Signals Platoon, the Riggers Section, the IT Section, the Technical Support Section and the Outpost Section. The Signals Platoon is headed by a Warrant Officer II and is made up of 34 AFM officials who work on a 12-hour shift (day/night/rest/off). The Signals Platoon manages and operates the Operations Centre AFM, which also doubles as an RCC or as a National Co-ordination Centre (NCC). It maintains an integrated maritime picture through radar and other IT driven systems. The Outpost Section in Dingli, Madliena and Delimara is responsible for Coastal Lookouts. Every Outpost Section is manned by a Lance Bombardier who must report for duty, via radio or telephone communication, to the Signals Platoon on the hour. The Riggers Section, headed by a Staff Sergeant, is responsible for the overall maintenance and upkeep of the communication masts. On the other hand, whilst the IT Section, headed by a Sergeant, is responsible for the overall support and the provision of IT Services, the Technical Support Section is headed by a Staff Sergeant and is responsible for the telephony, network support and infrastructural works.

2.2 IT Strategy

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

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

Consolidating the previous recommendations and consultations held between the previous AFM CIS representative, MITA and the IMU OPM in 2010 and early 2011, the Headquarters AFM CIS Section opted to follow the advice to move towards a *"Federated"* CIS architecture. Following this, in November 2011, a paper entitled *"Outlining the Armed Forces of Malta Communications and Information Systems Concept toward a Federated Environment"* was published. It identified two infrastructural elements that were deemed essential by the AFM to adopt a Federated model. The "Federated" model operates on the same lines as that adopted by other military organisations.

The AFM adopted a phased and incremental approach to identify and assess the risk, estimate the level of capabilities needed to address the identified risks, build and sustain the required levels of capability, develop and implement plans to deliver those capabilities, validate and monitor progress, and review and update efforts to promote continuous improvement. The two recommended projects are:

1. A Data Centre to host all the AFM CIS services, applications, networking and communications infrastructure, to ensure the availability, performance and reliability of CIS services in support of military operations and administrative functions;

2. The effective design and commissioning of an autonomous AFM Wide Area Operational Network architecture linking the Headquarters AFM, Operations Centre and all the AFM Units and their respective Sub-Units. It is envisaged that this network will then be extended further to include remote sensor sites and radar sub-systems located at strategic locations in Malta and Gozo.

2.3 AFM ICT Expenses

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

AFM ICT Expenses	Total Operational and Capital Expenditure
2012 (Actual)	€75,434
2013 (Planned)	€67,390

Table 3 – AFM ICT Expenses

As depicted in Table 3, the NAO observed that the Operational and Capital Expenditure planned for 2013 is €8,044 less than the previous year. The cost for the procurement of new PCs and laptops covered under the leasing agreement, the recurrent costs related to the fibre-optic connections at the AFM Luqa Barracks, the Servers' SLAs and MITA Core-services costs were funded by the IMU OPM. The planned ICT budget also includes the recurrent SLA costs related to the AFM Website, the DMS, and the SLA related to the Coastal Radio Station.

	Capital Expenditure	Operational Expenditure
Data Room Project	€490,644	€10,738
Upgrading of AFM WAN	€112,808	€49,885
Total	**€603,452**	**€60,623**

Table 4 - Planned ICT Expenses for 2013

In the meantime, the NAO was informed that a separate Capital and Operational Expenditure budget was planned for 2013 to cater for two core infrastructural projects, without which the AFM would not be able to assume a Federated model as highlighted in its IT Strategy. As depicted in Table 4, these two core infrastructural projects entails a new Data Centre to consolidate all the AFM services, applications, networking and communications infrastructure and to upgrade the existing AFM WAN with the required bandwidth to support the overall AFM operations and administration. The estimated costs and required plans for the new Data Centre were estimated by MITA's Facilities Management and Infrastructural Department, which were then forwarded to the IMU OPM for approval.

2.4 Systems Development Life Cycle

If standards are not in place and enforced in an IT environment, projects probably will be executed in an undisciplined fashion increasing the possibility of quality issues in the developed or purchased products, and causing the IT environment to be unnecessarily diverse. The latter will eventually cause an increase in support costs and potential interface and compatibility issues.

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

2.4.1 Hardware Asset Management

The Headquarters AFM Procurement and Logistics Branch is headed by a Colonel and is responsible to attend to the diverse logistical requirements of the force. The tasks it routinely fulfils vary between providing the requisite individual clothing and equipment for the soldiers, major procurement and subsequent maintenance requirements and schedules of the force's major operational equipment such as its fleet of aircraft, patrol vessels and vehicles and the overall IT assets.

The AFM Procurement and Logistics Branch focuses not only on satisfying the specific requirements to meet operational necessities but also on ensuring that its resources are procured, supplied and eventually used effectively, efficiently and economically or in simpler terms that its resources are used and applied as required to achieve the desired outcome.

2.4.1.1 Procurement

As stated earlier, all the procurement of IT assets, including the AFM CIS Resources, is governed by the Headquarters AFM Procurement and Logistics Branch. The NAO was informed that the AFM CIS Section had issued a specific policy related to the procurement of IT assets entitled *"AFM Standing Orders Section 45 – End User Support Policy"*. The latter states that the Headquarters AFM Branches, Sections and Units are to direct all purchase requests, based on a legitimate need, to the Headquarters AFM CIS Section, for PCs, laptops and peripheral devices such as printers and scanners including software packages.

Since the AFM was required to abide to the Government leasing agreement for the procurement of PCs and laptops, the old PCs and laptops used within the AFM were replaced by the third party supplier as per the PC Leasing agreement. Thus, all the PCs, laptops and peripheral devices procured or leased by the AFM conform to the GMICT policy published by MITA.

2.4.1.2 Maintenance

All the AFM IT equipment is maintained by the IT Section CIS Company 4th Regiment. The latter offers first line support, whereby all the users must submit all their requests for hardware and software support services to the IT Section CIS by e-mail, phone or in person.

In view that no servicing on all the AFM leased PCs and laptops is allowed by the IT Section CIS, in case of a hardware or software malfunction, the IT Section CIS raises a service request with MITA's Service Call Centre. In this regard, all the PCs and laptops are brought over to the IT Section CIS for on-site servicing by the third party contractor. The NAO was informed that an AFM technician is present at all times during on-site diagnoses performed by the third party contractor. If any extensive or specialised hardware repairs would be required off-site, at the third party contractor's workshop, the PC or laptop's hard disk drive is removed for safekeeping at the IT Section CIS. This will then be re-installed by the third party contractor when the PC or laptop is returned to the AFM.

During the course of this IT audit, the NAO observed that whenever a service request is raised with MITA, all the e-mail correspondence with MITA is stored in an offline mailbox, whilst a copy is kept in a file. The same procedure applies whenever a third party supplier is called upon to service an AFM owned IT application or servers. However, the NAO observed that the IT Section CIS does not record any incoming IT service requests. Thus, the IT Section CIS cannot quantify the amount of IT service requests raised internally on a daily basis. The NAO recommends that since the IT Section CIS offers first line support on all AFM Hardware and Software applications, all incoming internal IT requests, whether by phone, e-mail or in person, should be recorded electronically. If the latter were kept updated, the AFM would be able to analyse trends and calls of a particular nature, which collectively may indicate a common source. Furthermore, the amount of calls registered would substantiate the level of support being provided by the IT Section CIS across the AFM and would even help in human resources capacity planning and decision-making.

2.4.1.3 Disposal

During the course of this IT Audit, the NAO was informed that the disposal of items falls under the responsibility of the Headquarters AFM Procurement and Logistics Branch. The NAO is pleased to note that the AFM adheres to an internal procedure on the proper disposal of IT equipment.

In this regard, prior to the disposal of IT equipment, three copies of the Army Form General (AFG) 1045 template is completed at Sub Unit level by the Company Quarter Master Sergeant (CQMS) and forwarded to his/her Unit Quarter Master (QM). This form is used to request the services of the AFM CIS Section or a local private contractor to inspect and classify the Sub Unit IT equipment, which was reported as damaged. The three copies of the AFG 1045 form are forwarded to the Progress and Control (P&C), which forms part of the Staff Quarter Master (SQM) within the Headquarters AFM Procurement and Logistics Branch. A copy of the AFG 1045 template will be retained by the P&C, while the remaining two copies will be returned to the originating Sub Unit. The latter will then forward a copy of the AFG 1045 template and the IT equipment to the AFM CIS Section for inspection. In the event that the AFM does not have the technical expertise, a technical inspector from a local private contractor might be called in to classify the IT equipment or provide the necessary recommendations. In the meantime, the P&C issues an AFM F1084 'Job Card' for every job initiated. This form will contain information such as the job number, authority number and the description of the job/works required.

The technical inspector assigned within the AFM CIS Section or local private contractor will issue a statement or report, which would state whether the IT equipment could be repaired or else classified as Beyond Economical Repair or Beyond Repair. The final report and the inspected IT equipment are returned to the originating Unit QM, whilst a copy of the report is forwarded to the P&C. Upon receiving the report, the P&C will complete the Job Card, which will include the job completion date, the total hours taken to carry out the inspection/repairs of the IT equipment and any costs incurred.

Finally, a Condemnation Certificate is issued by the P&C, which is then forwarded to the Headquarters AFM Procurement and Logistics Branch for approval and endorsement. The endorsed Condemnation Certificate is forwarded by the P&C to the originating Unit, which is then presented to the Board of Survey when requested.

Once the above procedure is completed, the disposal of the IT equipment is carried out through the Board of Survey. The Unit QM will present the SQM with the IT equipment marked for disposal together with the Condemnation Certificate and the respective forms.

2.4.2 Software Asset Management

The NAO reviewed the project life cycle in terms of the software asset management. The NAO observed that every application in use within the AFM is either a legacy system or an open-source application upon which only a few enhancements were made.

The NAO was informed that the AFM carried out a system development life cycle process on the AFM HRMIS in which the AFM had commissioned MITA to custom develop a system based on AFM's business requirements. In this regard, the system development life cycle process adopted by the AFM included:

- A feasibility/requirement determination exercise;
- System design;
- Alpha and beta testing; and
- Commissioning stage.

The implementation of the AFM HRMIS included the procurement of a dedicated server, client software installation, administrator and end-user training and data migration. The AFM CIS Section ensured that all the training material and system documentation is easily available and any changes required to the system must conform to the change management processes.

The NAO observed that the *"AFM Section 41 – Part 1 – Infrastructure Hardening Policy"* stipulates that all the leased PCs and laptops in use within the AFM are installed according to the Government Standard software image and the published GMICT policies. Furthermore, the Headquarters AFM Branches, Sections and Units must forward a request to the AFM CIS Section to seek authorisation for additional software installations on the leased PCs and laptops. The request for additional software must be based on a legitimate business requirement. Requests are then forwarded to MITA for the provision of the software required. Any requested software application that is not included in the Government Enterprise Agreement must be properly licensed and procured as per the AFM financial regulations endorsed by the Colonel Procurements and Logistics.

2.5 PC Leasing Scheme

In 2008, the Government of Malta through the then Ministry for Infrastructure, Transport and Communications (MITC), embarked on the implementation of a PC leasing framework within the Public Service. The objective of this initiative was to have a more efficient and effective ICT service by implementing a programme which necessitates the replacement of existing equipment though the

deployment, under title of lease of PCs and laptops, as well as for the provision of maintenance and support services to all workstations across the Public Service.

Following the implementation of the PC leasing framework, the AFM replaced all the existing desktop computers and laptops. Since the leased desktop computers and laptops were relatively new, this scheme reduced much of the maintenance burden that previously fell on the IT Section within the CIS Company 4th Regiment.

Although this scheme brought about a number of benefits to the AFM, the NAO noted the following issues that were impacting the AFM:

- As highlighted earlier, the IT Section CIS offers technical first line support on all the IT equipment within the AFM. In the event that a PC or laptop is transferred to another user, the IT Section CIS will secure wipe the hard disk to ensure that no confidential data is present. In this regard, the IT Section CIS raises a request with MITA's Service Call Centre in order for the third party contractor to be called upon, and re-image the PC or laptop hard disk with the Government Standard software image. The same applies whenever there is a problem with the Windows Operating system and needs to be re-imaged. The NAO observed that every time the third party contractor is called upon, a service charge is applied for every PC or laptop hard disk serviced, since the IT Section CIS does not have the flexibility to install the Government Software standard image itself;

- The NAO recommends that the AFM should take steps to obtain the current changes and SLAs applicable to PCs and laptop maintenance. The AFM should also negotiate with MITA the possibility of installing the Government Software standard image when re-installing software on PCs and laptops.

2.6 IT Inventories

An IT inventory is critical for the implementation of an organisation's strategy. It usually involves gathering detailed hardware and software inventory information, which is then used to make decisions about hardware and software purchases and redistribution.

Having an IT inventory in place will help organisations manage their IT systems more effectively and saves time and money by avoiding unnecessary asset purchases and maintaining an updated list of existing resources. Any organisation that develops and maintains an effective IT inventory program further minimises the incremental risks and related costs of building IT infrastructural projects based on old, incomplete or/and less accurate information.

The NAO was informed that the IT Inventory falls within the remit of the AFM Procurement and Logistics Branch. Whenever a new item is procured, an internal procedure is adopted whereby the item is recorded on the Technical Equipment Account Ledger and assigned with a receipt voucher number issued from the Schedule of Vouchers of the current year. Subsequently, the account holder

presents the ledger to the QM to countersign on the ledger that the entry has been properly registered and recorded. All the items procured and classified as “Starred Items”, that is of tactical and technical value, are additionally registered in a Special Stores Register.

This process ensures that appropriate records exist when the item was procured and from which supplier, through the Local Purchase Order (LPO) reference number issued from the Accounting System. Furthermore, it also records to whom the item was issued (that is to which Sub-Unit) and whether the item has been assigned to some other unit or to the board of survey for condemnation or disposal.

Any IT asset procured is distributed to Sub-Units only through their respective CQMS. The Regimental QM account holder ensures that the pertinent CQMS collects the item and acknowledges both the issue of the item as well as the resultant balance per item of the Sub-Unit, by countersigning the pertinent ledger. The same procedure is applied to any items issued by the QM 4th Regiment (being the central AFM Account Holder on all IT-related items) to other units. In this scenario, the pertinent Regimental Technical Equipment Account holders of other units have to follow the same procedure and countersign the ledger for items issued to their respective unit.

Furthermore, any IT asset with a purchase value above the €100 threshold is also registered in the Accounting System. A further control measure is adopted at the respective unit level, through which the Sub-Unit CQMS at the various AFM units are obliged to send their respective Regimental QM Sergeant with a controlled Stores Certificate on a monthly basis. The latter confirms or otherwise the true balance and state of all the “Starred Items”.

The NAO observed that even though the AFM Procurement and Logistics Branch maintain the overall IT Inventory in a very efficient and structural way, the NAO recommends that the AFM should refine their current inventory process and invest in an electronic IT Inventory application whereby all assets are stored centrally.

In the absence of an electronic IT inventory application, the NAO observed that the IT Section CIS makes use of a software application, which offers amongst others a database inventory of all the AFM Windows servers and workstations. This application simplifies the administration of all the AFM workstations connected to the AFM Domain, whereby it extracts all the necessary system information, such as Computer name, network configuration settings, software applications, drivers and hotfixes installed in a centralised database.

2.7 Third Party Suppliers

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

The AFM has a Ministry wide contract with MITA that covers the Core Service items common to Government. In this regard, MITA provides the AFM with a Fiber-Optic or ADSL connection to MAGNET.

The ICT services contract also covers the 24/7 monitoring carried out on the MAGNET, namely on Core WAN equipment and Core Access Switches, to prevent potential ICT problems resulting in service downtime. Furthermore, MITA is also providing the AFM with a number of other services:

- E-mail;
- Internet browsing and filtering;
- Standard Desktop Security Configuration Services, such as Anti-Virus, Patch Management and spam filtering of e-mails via black lists and tagging;
- Access to MITA's Service Call Centre for the reporting of incidents related to the above services;
- Second line support for the resolution of incidents, reported to MITA's Service Call Centre regarding the above-mentioned services to leased PCs and laptops.

In this regard, the AFM informed the NAO that they do not have a copy of this service contract and do not have visibility on these contracts notwithstanding making specific requests to this effect. In fact, these contracts fall within the remit of the Chief Information Officer of the respective Ministry. However, the NAO recommends that the AFM should obtain a copy of this service contract.

The NAO also observed that in October 2012, the AFM signed a framework agreement with MITA to cover the delivery, management and execution of programmes related to the implementation of IT and Information Systems within the AFM Federated Model.

In the meantime, the NAO observed that the AFM has SLAs with the respective third party suppliers responsible for the Coastal Radio Station and the VTMIS, the electronic DMS and the AFM Back-end servers.

On the other hand, the ICS[1] is not covered by any SLA. When the two-year warranty elapsed in early 2011, no SLA was negotiated to cover the maintenance and servicing aspects of this system. The NAO was informed that the Headquarters AFM CIS Section is doing its utmost to try to establish an SLA with a local company. However, since the system has different modules, which were assembled from hardware provided by a number of foreign communication suppliers (in the United States, Australia and Israel), who had collaborated on the implementation of this system, the AFM are finding it very difficult to try to negotiate an SLA with one communications supplier. The NAO acknowledges the fact that the AFM are finding it difficult to establish an SLA, however unless there is a formal SLA it would be very difficult to rectify hardware faults or system operability issues, including system upgrades or hotfixes.

[1] Refer to Section 3.4 – Integrated Communications (Radio over IP) System

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. A network infrastructure provides the communication path and services between users, processes, software application services and external networks.

2.8.1 AFM Operational Wide Area Network

During the course of this IT Audit, the AFM CIS Section provided the NAO with a logical diagram of the WAN Architecture.

The AFM Headquarters, the Operations Centre and the 4th Regiment AFM, which are all co-located at Luqa Barracks, are connected to MAGNET via a 10 Megabits per second (Mbps) fibre-optic link to MITA-01 Data Centre in St. Venera. On the other hand, the AFM units, namely the 1st Regiment AFM (Ħal Far), the 3rd Regiment AFM (Safi), the Maritime Squadron (Pietà), the Air Wing (Luqa Airport), the Gozo Command (Qortin – Gozo) and the Air Defence and Fire Support Company (Luqa Airport) are individually connected to MAGNET through ADSL bridges as depicted in Figure 1.

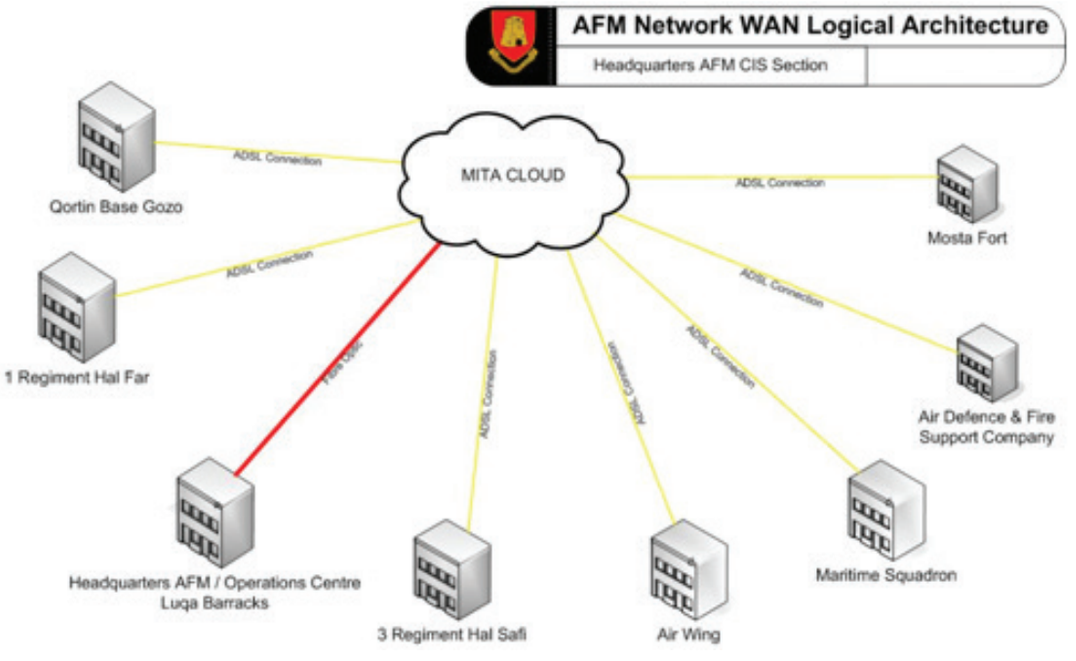


Figure 1 - AFM WAN Logical Architecture

The NAO was informed that since these separate data lines are physically aggregated at MITA, the current network configuration places severe bandwidth constraints on the AFM's administrative and operational information exchanges. This is attributed to two main underlying reasons:

1. The bandwidth speeds are extremely low, when compared to today's communication standards, because the physical bandwidth capacity of the telephone lines have reached its limits and cannot be upgraded any further;

2. Furthermore, since the AFM servers are hosted at Luqa Barracks, the CIS Services requested by the AFM Units outside Luqa Barracks, are routed through MITA equipment first before the AFM Units can access their own folders or application systems as depicted in Figure 1.

As part of the Core Services contract, all WAN equipment and Core Access switches are monitored and maintained by MITA on a 24/7. The AFM CIS Section is then notified by MITA whenever there is a service disruption. The NAO observed that the IT Section CIS has a monitoring console whereby the LAN infrastructure, the AFM Servers and the MCL network are visually monitored. Furthermore, the VTMIS network infrastructure, including the VTMIS servers, have a separate monitoring console. The VTMIS is monitored and maintained by staff of the IT Section CIS and supported through an SLA.

While reviewing the AFM network setup, the NAO observed that all networking equipment is connected to a Universal Power Supply (UPS). Ideally, every UPS has a network management card installed. The network management card provides a secure monitoring and control of the UPS via a web browser. This card will then be configured to send an e-mail notification on to the AFM CIS Section generic e-mail account in the event of a power disruption. The NAO noted that none of the UPS has a network management card installed even though a few UPSs support this card. In this regard, the NAO recommends that the AFM CIS Section should procure these network management cards and configure them as part of their monitoring tools.

In the meantime, all the data and communication rooms and the AFM Operations Centre are backed up by diesel-powered generators. The NAO notes with satisfaction that the AFM regularly monitor and test the UPSs and the diesel-powered generators on the 15th of every month by dedicated staff of the Pioneer Section within the 4th Regiment AFM.

2.8.2 AFM MCL Network

In 2001, the AFM had commissioned and operated an MCL Network. The latter is the core operational network infrastructure and communications backbone for the VTMIS, GMDSS Coastal Radio Station and ICS. Data and voice from remote sensors of the VTMIS (radar subsystems, radio antennas and Closed Circuit Television (CCTV) feeds) from sites located at key positions across Malta and Gozo are transmitted over the MCL Network to the AFM Operations Room. The remote sites are located at Delimara Lighthouse, Dingli, tal-Ġordan Lighthouse in Gozo, Ta' Sopu Command Barracks at Nadur

Gozo, Madliena Fort at Madliena, Safi Barracks, Ħal Far Barracks and Luqa Barracks. The data received from these remote sites is consolidated to present a comprehensive real-time representation of the vessel traffic situation.

The NAO was informed that the AFM MCL Network had reached technological obsolescence and could not be upgraded further. The microwave technology and hardware that is currently in use by the AFM has been phased out by the manufacturer and system spares are no longer available for procurement.

The NAO observed that the AFM IT Strategy highlights the importance of having an autonomous operational WAN, whereby the required bandwidth will eventually support the AFM operations and administration, which will incorporate all the AFM units including the remote sites' sensor nodes comprising the MCL network.

Chapter 3

IT Applications

Chapter 3

IT Applications

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

- AFM HRMIS
- Coastal Radio Station
- EUROSUR
- Integrated Communications (Radio over IP) System
- VTMIS

3.1 AFM HRMIS

The AFM HRMIS is a multi-user Management Information System through which data is inputted by the respective AFM Units. The NAO observed that viewing rights are given only to authorised users by the IT Section CIS System Administrators on a need-to-know basis.

The NAO noted that the HRMIS system was custom developed by MITA in 2001, according to the AFM business requirements, and followed the software development life cycle that consisted of:

- A feasibility/requirement determination exercise;
- System design;
- Implementation, beta testing and system documentation;
- Deployment and maintenance.

In the meantime, the NAO observed that programming manuals were not made available by MITA as per industry standard but the programming code was made available to the AFM. The NAO is pleased to note that the AFM were also provided with the system analysis documents, which entail all the database tables, fields and entity relationship schematics. To date, no changes in the overall table schemas or amendments in the document were required. Furthermore, user manuals were not made available, however, beta testing followed by intensive training was provided for the AFM officials. The end-user training was co-ordinated by the AFM Computer Section, which was responsible for IT matters at that time, as an integral part of the implementation process.

The NAO observed that all the AFM HRMIS user accounts (including all other applications' user accounts in use by the AFM) are governed by the AFM Standing Orders Part 1 Section 39 *"User Account Management Security Policy"*. Thus, all the requests for the creation, modification and deletion of the AFM HRMIS user accounts originate from the respective AFM Branches, Sections and Units on behalf of the users under their command. The AFM HRMIS has the required functionality to add users to pre-defined groups with pre-established user permissions.

The NAO observed that the AFM HRMIS does not adhere to password management best practices. In this regard, the AFM HRMIS does not offer any password complexity rules or any password length policy. Moreover, the AFM HRMIS user account passwords do not expire over a period number of days and the AFM HRMIS does not maintain any password history, to ensure that old passwords are not continually re-used. In the meantime, the NAO noted that if a user has forgotten his/her password, the AFM HRMIS does not offer the functionality to generate a new password. In this regard, the current HRMIS account is disabled by the System Administrator whilst a new account is created for the user. The creation of a new user account is not menu driven but all user accounts are embedded at the backend database. All the previous user profiles/groups will then be linked to the new account. Taking into consideration the criticality of the system, the NAO recommends that the AFM reviews the current password management process to ensure that best practices are applied to the AFM HRMIS system.

The NAO was also informed that the AFM HRMIS has a full audit trail functionality that records who, when, how and what files have been accessed or inputted into the system. Thus, the AFM HRMIS generates a secure audit record each time a user accesses, creates or updates data from the system. Moreover, the NAO observed that the end-users did not have access rights to delete any data and any deletions were performed directly on the Server Back-end. The NAO noted that such deletions were supported by a written request from the Regimental Headquarters or from the AFM Records Office within the AFM Personnel and Admin Branch. All the written requests were then forwarded to the AFM CIS Section.

During the course of this IT Audit, the NAO was informed that the AFM HRIMS underwent a number of enhancements and all known bugs were addressed over the years, with the result that the AFM HRMIS has reached maturity. In this regard, the AFM CIS Section took the decision not to include the system as part of an SLA and thus there is no contract in place. Even though the AFM HRMIS is maintained by the AFM CIS Section, in the event that some enhancements or a system upgrade is required, the AFM CIS Section will then contact the third party supplier who in return will offer his/her services on a time-and-material and best effort basis.

The NAO noted that the AFM HRMIS is backed up daily to disk, from Monday to Thursday, on to the AFM Backup server, according to the internal Business Continuity policy entitled *"Policy Governing the AFM CIS Business Continuity Aspect for Servers and Application Servers"*. Apart from the daily backups, the AFM HRMIS is also backed up to tape according to the *"grandfather-father"* rotation scheme, whereby a full monthly backup ("grandfather") is scheduled on the first Friday of the month whilst a full weekly backup ("father") is scheduled on the remaining Fridays of the month. In the meantime, all backup media are securely stored off-site in a safe. The latter is only accessed by the AFM CIS Section Commanding Officer and his assistant. For accountability purposes, the IT Section CIS System Administrators have to sign their names whenever a backup tape is issued or returned from the safe.

Although the AFM monitors the daily backups to ensure that the backup has been completed successfully, the NAO was informed that the backups are not being tested. This goes against the internal *"Standing Operating Procedures – Backup and Recovery of Systems, Application and Data Servers"* which stipulates, *"The CIS Company 4th Regiment is required to perform periodic test restores of the system to ensure the proper functioning of the backup processes. The maximum interval between test restores is quarterly"*. Since the AFM HRMIS is a critical application that caters for the AFM payroll and the maintenance of AFM personnel data including medical records, the NAO recommends that the AFM should perform test restores periodically to ensure that data can be retrieved from the current backup lifecycle if and when the need arises. In the meantime, the NAO was informed that the AFM CIS Section is currently liaising with MITA to set up a replicated HRMIS environment at MITA-01 Data Centre in the near future. In this regard, it is envisaged that a full data restore exercise is carried out jointly between the AFM and MITA.

3.2 Coastal Radio Station

Since 2009, the AFM has operated a Maritime Coastal Radio Station to conform to the GMDSS safety engine. The GMDSS is an internationally accepted set of safety procedures, including types of equipment and communication protocols used to increase safety and facilitate the rescue of distressed ships, boats and aircraft.

The GMDSS consists of several systems, which are intended to perform a number of functions, such as alerting (including position determination of the unit in distress), search and rescue co-ordination, locating (homing), maritime safety information broadcasts, general communications and bridge-to-bridge communications.

The AFM Operations Centre plays a number of roles in this respect. Primarily, it is the Malta Search and Rescue Co-Ordination Centre both for maritime as well as aeronautical incidents. The Search and Rescue Co-Ordination Centre is designated as the National Search and Rescue point-of-contact, to which all the related information and requests are directed to. The RCC is responsible for the co-ordination of any Search and Rescue incident within the Malta Search and Rescue Region as depicted in Figure two.

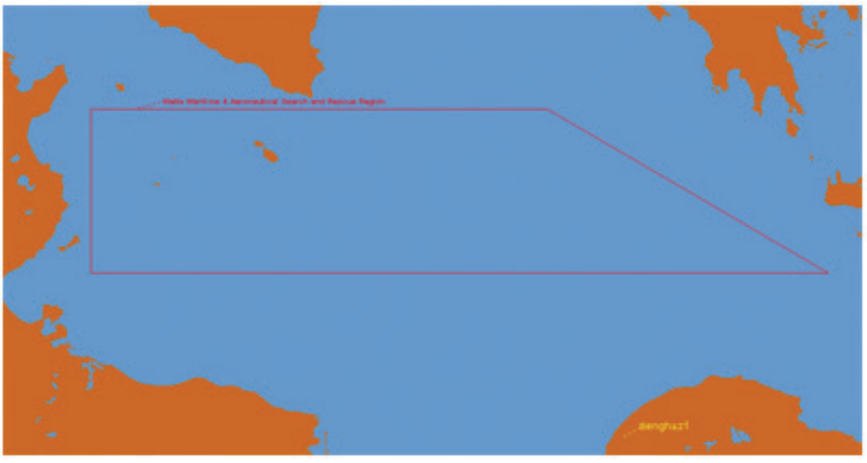


Figure 2 - Malta Search and Rescue Region

To accomplish these functions, the AFM officials within the RCC are trained to high standards based on the United States Coast Guard techniques and utilise sophisticated Search and Rescue planning software, developed by the same United States Coast Guards. This was taken into consideration during the procurement process of the AFM's vessels and aircrafts to ensure full compatibility, to such a degree that plans developed on this planning tool are compatible with the navigation systems installed on the AFM's patrol boats and aircraft.

Apart from the RCC, the AFM Operations Centre also takes the role of the Malta Coastal Radio Station. In this regard, a continuous listening watch is maintained on international distress radio frequencies in the Very High Frequency (VHF) and Medium Frequency (MF) bands. These communication means cover up to 20 nautical miles and 200 nautical miles respectively. Moreover, the Malta Coastal Radio Station transmits distress and safety related messages on the Navigational Telex (NAVTEX) system, which is received as text messages on board ships travelling through the service area covered by Malta as depicted in Figure three.

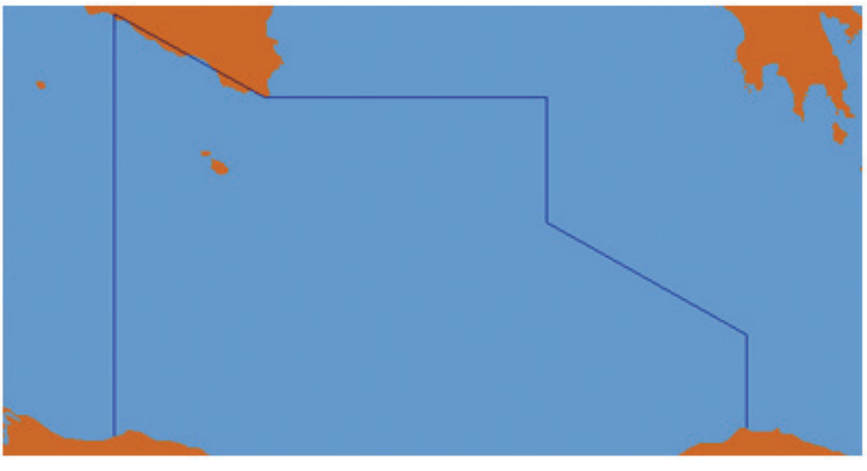


Figure 3 - Malta NAVTEX Service Area

NAVTEX is an international, automated system for instantly distributing maritime safety information, which includes navigational warnings, weather forecasts and weather warnings, search and rescue notices and similar information to ships. The system mainly operates in the MF radio band just above and below the old 500 kHz Morse Distress frequency and is utilised mainly by those countries with relatively small areas of coastline and/or sea areas to cover. A small, low-cost and self-contained 'smart' printing radio receiver is installed on the bridge or the place from where the ship is navigated, and checks each incoming message to see if it has been received during an earlier transmission. A similar 'smart' print radio receiver is also installed at the AFM Operations Centre.

During the course of this IT Audit, the NAO observed that the Malta Coastal Radio Station was integrated with the VTMIS. In this regard, in 2008, the same foreign supplier responsible for the VTMIS was invited by the AFM to submit proposals for the implementation of the Coastal Radio Station to cover the supply, delivery, installation, testing and implementation of the equipment for the operation of a digital selective-calling Coastal Radio Station. As highlighted earlier, the system provides all the functionality for distress and safety operation of Digital Selective Calling (DSC) on VHF and MF bands, VHF and MF radiotelephony for ship-shore and shore-ship communications, navigational warnings and weather forecast. The latter are periodically received via e-mail by the Malta International Airport up to 100 nautical miles. In return, the AFM will then transmit the weather forecasts through NAVTEX.

All activities of the Malta Coastal Radio Station are remotely controlled from the AFM Operations Centre at Luqa Barracks via the AFM MCL network connecting remote communications and IT subsystem sites located at key sites across the Maltese Islands. Thus, the Malta Coastal Radio Station's main hub is located at the AFM Operations Centre in Luqa, and the antenna and Back-end transmitters were installed at the AFM Safi Barracks. On the other hand, the AFM Outposts in Madliena was equipped with DSC receivers on MF bands, whilst the AFM Outpost in Dingli and tal-Ġordan in Gozo were equipped with DSC receivers on VHF bands.

Since the Malta Coastal Radio Station is supported by the same suppliers responsible for the VTMIS, whenever technical assistance or system maintenance is required, the IT Section CIS will then raise a service request with the foreign supplier as per the SLA in place. The foreign supplier system engineers will either resolve the matters online or else raise a service request with the local representative who in return will contact the AFM accordingly on any hardware related issues. The NAO observed that each reported incident and the respective e-mail correspondence are properly kept in a file. In this regard, a Failure Report Form is used to document everything in writing. Such form includes a log of the problem recorded, the log number allocated and the response time of the local supplier. The latter then provides all the necessary details in the Failure Report Form on how the problem was resolved to close off the incident, which in turn needs to be counter signed by the AFM.

Moreover, both the foreign third party supplier and the local representative adhered to the SLA agreed upon whereby full system maintenance is carried out yearly by the foreign third party supplier, whilst the local representative carries out a preventive or corrective maintenance every quarter. To date, the AFM is satisfied with the response time and the level of support being offered by the respective suppliers. The foreign third party supplier provided the AFM with user manuals and system documentation, which are continuously being updated. End-user training was provided while the

system was being implemented. The AFM adopted the train-the-trainer approach through which user training was provided on the job to other AFM officials.

3.3 EUROSUR

In the amendment to Frontex Regulation (EU) 1168/2011, the European Parliament and the Council tasked Frontex[2] *"to provide the necessary assistance to the development and operation of a European border surveillance system and to the development of a common information sharing environment, including interoperability of systems"*.

The EUROSUR[3] system aims at increasing co-ordination within and between Member States, with the exchange of operational information, to reinforce border surveillance, prevent and tackle serious crime, such as drug trafficking and the trafficking of human beings. The increased exchange of information and the use of modern surveillance technology introduced by EUROSUR can be vital for saving the lives of migrants attempting to reach the shores of EU Member States in small and unseaworthy boats that are very difficult to track and thus helps to diminish the unacceptable death toll. The use of the EUROSUR tools is strictly conditioned to the respect of fundamental rights and in particular the principle of non-refoulement.

The EUROSUR system establishes a permanent connection among EU member states and Frontex to provide a fully extensible information sharing system for both non-classified as well as classified information. For this purpose, each Member State with land and maritime external borders will establish a NCC, also referred to as EUROSUR Nodes. The exchange of information is based on multilateral agreements that may be made between any pairs of NCCs and between NCCs and Frontex. In this regard, the NAO was informed that the AFM is the local designated national authority on integrated maritime surveillance and the Malta EUROSUR node and Back-end infrastructure is located at the AFM Luqa Barracks.

The possibility for exchanging personal data in EUROSUR is very limited. At European level, Member States and Frontex is limited to operational information, such as the location of incidents and patrols, and analysed information such as ship identification numbers. Any exchange of personal data between Member States and third countries is strictly limited to what is necessary (for example to identify a boat in distress) and is carried out in line with EU and national data protection rules.

Thus, the exchange of information in the framework of EUROSUR takes the form of 'situational pictures', which can be described as graphical interfaces presenting data, information and intelligence. These 'situational pictures' are established at national and European level and are structured in a similar way to facilitate the flow of information among the EU Member States.

In order to improve the capability to detect small vessels, Frontex implemented a service for the common application of surveillance tools, combining, amongst other things, satellite imagery with

[2] http://www.frontex.europa.eu

[3] http://europa.eu/rapid/press-release_MEMO-13-578_en.htm

information from ship reporting systems. This service increases the possibility of identifying and tracking down the routes used by criminal networks. The fact that traffickers are currently using small wooden and glass fibre boats for smuggling both human beings and illicit drugs poses a major challenge to law enforcement authorities because it is extremely difficult to detect, identify and track such small boats on the high seas.

Once the 'situational pictures' are made available to the relevant actors, it is for Member States to decide upon follow up measures, including interception of boats suspected to carry out criminal activities or rescue at sea in case of emergencies. When using EUROSUR, all Member States are bound by clear rules that guarantee full respect of fundamental rights, including the principle of non-refoulement. This also applies in case of co-operation between Member States and third countries in the framework of EUROSUR.

In December 2012, the EUROSUR Technical Office (ETO) set up the EUROSUR Hardware infrastructure and commissioned the application within the AFM, since the AFM is the designated national authority on integrated maritime surveillance. At the time of the IT audit, the NAO observed that the AFM could not officially utilise the EUROSUR application, as this was still a pilot project among the EU Member States. However, in October 2013, the EU Council adopted the regulation[4] establishing the EUROSUR system as one of the key tools at its disposal to prevent any tragedies at sea. The EUROSUR regulation will apply to the member states located at the Southern and Eastern external borders from 2nd December 2013 and to the remaining member states from 1st December 2014. The approval came into force a week after a boat full of asylum seekers, mostly from Eritrea and Somalia, sunk just off the coast of the Italian island of Lampedusa, whereby at least 289 people drowned and only 155 survived. The NAO recommends that the AFM monitors the outcome of this regulation and ensures that the AFM has enough resources that are familiar with the use and the daily monitoring of the EUROSUR system.

When the EUROSUR system was commissioned by the ETO, all the system documentation was handed in to the AFM CIS Section. Frontex also provided the AFM with user manuals with updated versions. In the meantime, two AFM officials attended training on the EUROSUR application abroad at the Frontex Headquarters in Warsaw, Poland. In return, the two AFM officials adopted the train-the-trainer approach whereby user training was provided on the job to other AFM officials.

The NAO observed that all the EUROSUR user accounts are governed by the AFM Standing Orders Part 1 Section 39 *"User Account Management Security Policy"*. Thus, all the requests for the creation, modification and deletion of EUROSUR user accounts must originate from the respective AFM Branches, Sections and Units on behalf of the users under their command. The NAO noted that whenever a user account password is changed, the end-user must change their password upon first logon. However, there is no password complexity rule in place. Moreover, the EUROSUR system does not enforce any password expiry, password lockout or password history policy. The NAO was also informed that the system does not offer any audit trail functionality to view who, when, how and what files have been accessed or inputted into the system. However, the ETO had informed all the NCCs, including the AFM

[4] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/139099.pdf

that the next stage of the project will focus on the security aspect of the EUROSUR system. The NAO recommends that the AFM should ask Frontex for further information on the next stage of the project, during future technical meetings.

With reference to the Business Continuity aspect, the AFM adheres to the *"Policy Governing the AFM CIS Business Continuity Aspect for Servers and Application Servers"* whereby the EUROSUR system is backed up daily. Since all the EUROSUR services in the node are running on virtual machines, the EUROSUR system was configured to automatically execute a nightly snapshot of all virtual machines, which are then saved and backed up to disk on the AFM backup server. Even though the AFM monitors the daily backups to ensure that the backup has completed successfully, Frontex are also monitoring the system backup remotely, since EUROSUR is owned exclusively by Frontex.

In the meantime, all the EUROSUR hardware equipment and the network infrastructure was provided by Frontex and commissioned by the ETO. The AFM were provided with a monitoring console to ensure the smooth running of the system. In the event that a particular node is down, the AFM will liaise accordingly with the local communications service provider. On the other hand, the ETO will monitor the Malta node and will liaise with the AFM in the event of connectivity problem or software maintenance and enhancements are required.

The NAO was informed that the EUROSUR system contrary to the recommended synchronous fibre-optic connection is running on an ADSL internet connection with a local communications service provider. Moreover, to-date the AFM does not have a redundant internet connection to this node. In the meantime, the EU participating member states, including Malta, were informed that Frontex intends to provide a redundant cabinet in the near future, equipped with all the necessary IT Hardware components. The NAO noted that the current site of the Data Room, used for hosting the EUROSUR system, does not have sufficient space for the redundant cabinet mentioned above. On another note, the new site earmarked for the consolidation of the AFM servers and equipment, as highlighted in the IT Strategy[5], will have the required space.

3.4 Integrated Communications (Radio over IP) System

The basis of any operation is the ability to pass information between participating units in a timely and secure manner. Within the military, such ability assumes even greater importance given the sensitivity of the activities being conducted and the relevance thereof to the security of the state.

In meeting the challenge for more reliable communications over the years, the AFM implemented a number of phased changes to increase the ability to exercise command and control of AFM units, regardless of where they are deployed. These improvements were driven to a significant degree by the fact that AFM units were being deployed further afield in support of both national and overseas deployments. Activities within the international field, especially joint border control operations, also demonstrated the importance of operating communication systems that could support interoperability with those of the partners with whom the AFM was engaged.

[5] Refer to Section 2.2 – IT Strategy

In light of these considerations, an internal study was initiated to evaluate the ability of modern technology to provide the AFM with an integrated, secure and interoperable communications infrastructure. This would support the need to system growth and upgrades, as well as interoperability with legacy equipment and systems operated by international partners. The result of this study was a system concept that was referred to as ICS and envisaged a flexible core infrastructure designed to provide maximum capability.

The next step involved identifying funding to support the procurement of the system. The AFM decided to incorporate the project into the submissions made by the AFM under the External Border Funds (EBF) of the EU. The submission was considered favourable, and the project was allocated funding from the 2007 EU programme. As a result, the AFM were in a position to launch a competitive bidding process that saw a foreign company being awarded a contract in early 2009. Within eight months, the foreign company together with their local partners managed to implement an aggressive design, procurement and installation schedule, which transformed the ICS concept into reality.

Based on components of Australian, Israeli, European and United States origin, the ICS was installed aboard selected vessels, vehicles and aircraft within the AFM, as well as being available for use by individual soldiers. In conjunction with the fixed infrastructure and mobile command elements, the system allows secure (encrypted) radio communications. However, the ICS is not limited to voice communications but it permits the transmission of data, including documents, written orders, pictures and in some cases video, thus making it a critical enabler supporting both national and international operations. The ICS thus offers the tracking of AFM units when deployed, permitting command elements to have constant situational awareness and thus deploy resources in the most efficient and effective manner.

Apart from a secure radio communications, the ICS offers Radio over IP technology, whereby the system permits disparate communications systems to be brought together into a single operational network, which can also include non-radio frequency systems such as landline telephones and computer networks.

During the course of this IT Audit, the NAO observed how the AFM Operations Centre operates and manages the ICS. The AFM Operations Centre works on a 12-hour shift (day/night/rest/off), whereby in every shift, the AFM Operations Centre carries out visual inspections and a number of voice checks on the ICS equipment to ensure that every piece of equipment is in order. In the event of a hardware malfunction, this is written in the *"AFM Shift Handing/Taking over Sheet"*, which is exchanged in the change of shift. Moreover, an e-mail is sent to the local representative for technical assistance and the AFM Warrant Officer II in command of the AFM Operations Centre is informed accordingly.

Furthermore, since the ICS does not record any audio transmissions, the AFM Operations Centre records every incident or piece of information received or transmitted over the ICS in a logbook. The latter keeps track of all the communications, which include the date, time, if the AFM Assets (Aircraft, Vessels or Vehicles) were deployed in a Search and Rescue Operation, internal communications between the AFM Operations Centre and the AFM Outpost Sections (Delimara, Dingli and Madliena) etc.

The NAO is pleased to note that the AFM has a number of Standard Operating Procedures (SOPs) on the use of the ICS. These SOPs include amongst others how to reboot the ICS equipment in sequence, or how to transmit data/images in .XML format from the AFM Operations Centre to an AFM vessel out at sea through VHF radio transmission.

The NAO observed that the ICS main hub is situated at the Headquarters AFM Luqa Barracks whilst the ICS redundant equipment was installed at the 1st Regiment AFM in Ħal Far. Furthermore, the NAO noted that the AFM Mobile Unit is also equipped with the ICS equipment in the event of a system crisis, whereby both the AFM sites in Ħal Far and Luqa Barracks are unreachable.

During the course of this IT Audit, the NAO observed that the ICS was covered by a two-year warranty, which expired in 2011. Unfortunately, no SLA was negotiated on system commissioning to cover maintenance and servicing aspects of the system. In this regard, the AFM are experiencing a number of delays to rectify hardware faults and other system operability issues, including software updates and upgrades. To date, a local representative is providing system support and maintenance without any defined service levels in place. Thus, in the absence of a formal SLA, the service levels are slow since the different modules of the ICS were assembled from hardware provided by different foreign communication suppliers who had collaborated on this project.

However, in 2013, the AFM CIS Section carried out a post-implementation study on a number of issues that emerged over a number of months, following the expiry of the ICS two-year warranty. The study highlighted the following:

- The MCL network requires additional bandwidth to support the information exchange requirements of the system;

- A low user confidence in the usability of the system permeates across the board with operators preferring to operate legacy radio equipment. Furthermore, there are also no trained support personnel from the IT Section CIS to support the day-to-day running of the system;

- The negotiation of an SLA preferable with the local representative remains critical.

Following the above study, the NAO is pleased to note that the AFM CIS Section has identified two lines of actions to address the above issues:

- **Training** – Training courses were scheduled for System Administrators and the end-users. In this regard, the AFM will adopt the train-the-trainer approach, which must be concluded by the end of 2013. In total five training sessions were scheduled, whereby one training session intended for the IT Section CIS System Administrator and support staff was concluded by the end of August 2013;

- **Service Level Agreement** – The AFM CIS Section is currently negotiating an SLA with the local company, which was involved in the implementation of the ICS.

The NAO acknowledges the effort being made by the AFM CIS Section to negotiate an SLA at this point. On the other hand, this should have been negotiated during the ICS commissioning stage. Even though the AFM has redundant equipment, one small malfunction in the ICS might be critical in the overall running of the system. Thus, an SLA should cover at least:

- A description of the services being offered;
- The methods through which the services will be offered;
- The criteria through which delivered services will be measured;
- The quality standards of the services offered; and
- The line of action in case of failure of delivery.

In the meantime, the NAO was informed that the ICS is planned for extension after 2015 as part of an EU Internal Security Funding project. In this regard, further to the post-implementation exercise, the NAO recommends that the AFM should address any technical or operational issues and whether the ICS can cater for the recordings of all modes of transmission for any future playbacks.

3.5 Vessel Traffic Management Information System

In meeting the requirements stemming from the European Directive 2002/59/EC, the AFM is operating a coastal VTMIS. This directive came into force on 27th June 2002, as part of the action taken in line with the Commission's second communication on maritime safety following the Erika disaster. In this regard, the setting up of an EU VTMIS helps to prevent accidents and pollution at sea and to minimise their impact on the marine/coastal environment, and on the economy/health of local communities.

Thus, the aim of the VTMIS is to establish a community-wide vessel traffic monitoring information system with a view to enhancing the safety and efficiency of maritime traffic, improving the response of authorities to incidents, accidents or potentially dangerous situations at sea. It also caters for search and rescue operations and contributes to a better prevention and detection of pollution by ships.

The VTMIS is mandatory to commercial shipping and the port community through international and EU legislation. The VTMIS is complimented by the electronic port notification and ship clearance system (Portnet Malta) that operates over the Internet. All players within the port community, including terminal operators and other service providers, have access to the Portnet Malta on a need to know basis.

Whilst Transport Malta, which is the National Competent Authority (NCA) for ensuring the implementation and provisions of the Regulations (LN 458 of 2004 Territorial Waters and Contiguous Zone Act), operates the Ports Vessel Traffic System (VTS) and Portnet Malta, the AFM is the operator of the Coastal station VTS on behalf of Transport Malta. The Ports VTS and the Coastal VTS stations have the capacity for the exchange of information and replace the previous service provided by the Palace Tower Signal Station, commonly known as Turretta.

The NAO observed that the VTMIS project was implemented in two parts. Whilst phase one of the project, being the Port VTMIS, was co-funded by the EU National Pre-Accession Programme 2003, phase two involved the coastal VTMIS, which was co-funded by the European Regional Development Fund 2004-2006. Different foreign consortia represented by two local suppliers were commissioned to implement and maintain the respective VTMIS projects. The VTMIS project also catered for end-user training, which was provided to the AFM officials within the AFM Operations Centre, together with the relevant system documentation and user manuals.

Since February 2006, the AFM has operated the Malta Coastal VTMIS that provides 24/7 maritime surveillance and monitoring to help curtail illegal activities at sea, as well as to assist the AFM in their search and rescue services operations and border management control. The VTMIS configuration includes high performance coastal surveillance radars, radio direction finders, weather stations, an Automatic Identification System (AIS) base station network, digital CCTV Security System, a central control room at the AFM Operations Centre and other ancillary equipment. The VTMIS also sends automated ship notifications to the European Maritime Safety Agency through the National Safe Sea Net, which is obligatory to all EU member states.

The NAO observed that the operational hub of the Malta Coastal VTMIS is located at the AFM Operations Centre in Luqa, whilst the AFM Outpost sections in Fort Madliena, Dingli and tal-Ġordan Lighthouse in Gozo were equipped with VHF and HF receivers. In this regard, the NAO noted that the central infrastructure is connected to the Internet with a security appliance installed at the network perimeter. The Internet connection is required for remote support and for the publishing of an outward-facing web application. The security appliance, which provides the remote access facilities, is managed by the foreign third party supplier, whilst the AFM were provided with a password with which they can gain access to the device. Finally, the network hosting the VTMIS is connected through a dedicated network connection supplied by a local service provider.

During the course of this IT Audit, the NAO observed that all the VTMIS user accounts are governed by the AFM Standing Orders Part 1 Section 39 *"User Account Management Security Policy"*. Thus, all the requests for the creation, modification and deletion of the VTMIS user accounts must originate from the respective AFM Branches, Sections and Units on behalf of the users under their command. The requests are then managed centrally by the AFM CIS Section. The NAO observed that since the VTMIS application does not prompt the user to change their password upon first logon, the user must change their password from the VTMIS management console. In other words, whenever a user raises a password change request, the IT Section CIS System Administrator has to logon to the VTMIS management console and the user must physically change their password from the Administrator console. Furthermore, the NAO observed that the VTMIS does not enforce any password complexity, password expiry, and password lockout or password history policy. The NAO was also informed that the system does not offer any audit trail functionality. In this regard, the NAO recommends that even though the users cannot delete any data from the system, having an audit trail is fundamental to view who, when, how and what files have been accessed or inputted into the system. Ideally, the VTMIS system should also offer password policies as highlighted above and more efficient password management functionality.

In the meantime, the NAO was informed that a complete system upgrade on the existing hardware and software is planned by Transport Malta together with the AFM. In this regard, the NAO recommends that the AFM should co-jointly plan with Transport Malta and monitor this system upgrade beforehand, to ensure business continuity and that user training is provided if the software upgrade would entail in different operating procedures.

In the event that the AFM requires technical assistance on VTMIS, the AFM Operations Centre, as the first point of call, will raise a service request with the foreign third party supplier. The service request is then followed up by the IT Section CIS. Since the foreign third party supplier does not have access to the live system, a service request is raised with the local representative who will contact the AFM whenever technical assistance or system maintenance is required. The NAO observed that each reported incident and the respective e-mail correspondence are properly kept in a file. In this regard, a Failure Report Form is used to document everything in writing including the problem recorded, the log number allocated and the response time of the local supplier. The Failure Report Form will contain all the necessary details on how the problem was resolved by the local contractor. The form would need to be counter signed by the AFM in order to close the incident.

The VTMIS is covered by an SLA that entails three different types of maintenance, namely preventive, corrective and control maintenance:

- **Preventive maintenance** is mainly concerned with the physical infrastructure and all the supporting components. To ensure compliance with the overall hardware performance, the SLA states that every six months, qualified personnel will carry out hardware maintenance, which include the visual checks and cleaning of all the VTMIS equipment and maintenance on the air-conditioning system where the VTMIS equipment is located. Whilst preventive maintenance is carried out on the diesel generators, corrective maintenance is carried out yearly to check the foundation of the mast, antennas, earth connection and lightning protection amongst others.

- **Corrective maintenance** deals with the failure reporting, analysis and rectification of a problem. Should a failure occur, then a level would be assigned to the failure as follows:

    - Disastrous and Critical failures: the supplier and the AFM will rapidly establish and agree a Remedial Action Plan, with the aim to recover the system as quickly as possible according to the response time defined in the SLA;

    - Marginal and negligible failures: Such failures will be eliminated as soon as possible, taking into account the impact of the failure;

    - Implementation of Fixes: These will be made at the suppliers' discretion and in agreement with the AFM, which may include remote access tools such as Virtual Private Network (VPN).

- **Control maintenance** is concerned with the software components of the system whereby the first level of support is provided by the AFM Operations Centre with the daily monitoring, software diagnostics and corrective actions when necessary. Every quarter, the supplier carries out a number of health checks on the software components, whilst on-site software maintenance is carried out yearly to install updates, software patches or resolve any outstanding problems.

In the meantime, the NAO observed that the VTMIS has a pre-configured backup schedule covering a period of 28 days, until the cycle starts all over again. In this regard, the AFM CIS Section took the initiative to configure the AFM Backup server to copy the VTMIS backup folder to disk from Monday to Thursday and a Weekly Full System Backup on a Friday according to the "Policy Governing the AFM CIS Business Continuity Aspect for Servers and Application Servers". In the meantime, the NAO is pleased to note that the AFM CIS Section has a dedicated "Standing Operating Procedures on the Backup and Recovery of VTS Information". This SOP covers a number of procedures on how to backup the system, on how to monitor the backup logs and the actions to be taken in the event of a backup failure. The NAO observed that the AFM CIS Section performs periodic test restores of the system to ensure the proper functioning of the backup processes. Furthermore, all the VTMIS backup tapes are labelled accordingly and securely stored offsite.

Apart from the daily monitoring of the VTMIS backups, the AFM CIS Section has a monitoring console to ensure that all the VTMIS Servers and equipment are up and running, including the radar links at the AFM Outposts in Madliena, Dingli and tal-Ġordan in Gozo. Furthermore, the AFM CIS Section ensures that all the data rooms where the VTMIS equipment is installed are kept clean and free from clutter, whilst the temperature and humidity levels are kept constant.

Chapter 4

Information Security

Chapter 4

Information Security

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

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

The NAO analysed whether the AFM 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). 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, such as the AFM, and if everyone treats the same piece of information differently, this might have some major 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;
- How one can distribute information; and
- To whom this information may be disclosed.

In this regard, the NAO was informed that a *'Security Classification'* of documents or files is in place within the AFM. This standard is applied to all data or information that is created, collected, stored or processed within the AFM. All the data is then assigned one of the following classifications:

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

Depending on the level of classification, there are different rules controlling the level of clearance needed to view such information, how it must be stored, transmitted and destroyed. In this regard, the NAO was informed that the level of clearance adopted is linked to the official military rank within the AFM. Thus, if one takes into consideration the four levels of classification highlighted above, the AFM officials that would have the authority to classify any piece of information are:

- **Top Secret** – Lieutenant Colonel and above;
- **Secret** – Majors and above;
- **Confidential** – Captains and above;
- **Restricted** – All AFM officers.

It is to be noted that the data owners are responsible for appropriately classifying data and to comply with data use requirements. Hence, data that has been classified to particular level, can only be 'downgraded' with the authority of the originator.

4.1.2 Retention and Storage of Data

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

During the course of this audit, the NAO noted that the AFM holds a considerable amount of sensitive personal data and would thus like to highlight that the Data Protection Act makes specific provisions for sensitive personal data.

In this regard, the NAO was informed that the AFM does not have an official Data Retention and Storage policy. However, the AFM adheres to the Data Protection Act 2001, Chapter 440 of the Laws of Malta, and the related legal notices, whereby the processing of personal data must be:

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

As highlighted earlier, since the AFM does not have an official Data Retention and Storage policy, the NAO recommends that:

- A Data Retention and Storage policy is formalised and distributed to all concerned parties;
- The AFM Data Protection officer reviews the notification submitted to the Commissioner of Data Protection and ensures that the details within it are still applicable and if not update it accordingly;
- An owner is identified for every piece of personal data being held by the AFM; and

- The AFM Data Protection officer builds and maintains a register listing all the data being held by AFM, record when the data was collected, who has access to this data and when it will be disposed off.

4.1.3 Disposal of Information

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

As stated earlier, if confidential information is disclosed or lost could cause harm or distress. This includes personal data as defined by the Data Protection Act, that is information about a living individual where that individual could be identified, and other valuable or sensitive information to the AFM, which is not in the public domain.

The NAO is pleased to note that the AFM CIS Section had drafted a policy entitled *"AFM Standing Orders – Section 45 – End user support policy"*, which clearly explains how electronic data is being handled and disposed of. This policy states that whenever a PC or laptop needs to be replaced, the user's data will be transferred from the old computer to the new one by the IT Section CIS. The data will be retained on the old hard drive for one week after replacement to ensure complete data transfer. After one week, the hard drive from the old computer is securely erased or otherwise destroyed so that no data can be recovered from that drive. Similiarly, if a PC or laptop is to be reassigned to someone else, the hard disk is securely wiped by the IT Section CIS. The Service Contractor is then called upon to re-image the PC or laptop with the Government standard software package.

However, since this policy caters for only one type of media, the NAO recommends that a new policy be drafted by the AFM CIS Section to cater for the disposal of information on all types of media. Thus, this policy should clearly explain the procedure to be adopted on the disposal of any confidential information, which may reside on paper, flash memory devices, magnetic tapes or optical media, through shredding, secure wiping, demagnetising, physical destruction etc.

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 the plan is to recover lost data and to recover computer operations from any loss of data. This might entail a simple restore of lost or corrupted data or a full system restore due to a hardware malfunction or a complete loss of computer operations because of fire.

The NAO is pleased to note that the AFM CIS Section had drafted a policy, entitled *"AFM Standing Orders – Section 44 – Policy Governing the AFM CIS Business Continuity Aspect for Servers and Application Systems"*, which defined the strategy on how the AFM information and software application systems

are backed up. This policy applies to all the AFM systems, application and database servers and does not apply to end-users PCs, laptops and any peripheral devices. As a result of this policy, the AFM CIS Section drafted two different Standing Operating Procedures, namely a *"Standing Operating Procedures on the Backup and Recovery of Systems, Application and Data Servers"* and a *"Standing Operating Procedures on the Backup and Recovery of the VTMIS"*.

The NAO observed that the AFM CIS Section is responsible for the implementation of the servers' backup and restore processes. These tasks include the overseeing of the actual backup, the proper loading of tapes, tape storage and tape retention periods. In this regard, a dedicated backup software application, was installed and configured on the AFM Backup Servers, to perform an automated full backup to RAID (Redundant Array of Independent Disks) disks or to tape. The NAO observed that the AFM adopted the *"grandfather-father-son"* rotation scheme, whereby a full monthly backup ("grandfather") is scheduled on the first Friday of the month whilst a full weekly backup ("father") is scheduled on the remaining Fridays of the month. On the other hand, a full backup to RAID disk ("son") 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 these are labelled and kept off-site in a secure safe.

The *"father"* (weekly backups) set provides a retention period of one month, whilst the *"grandfather"* (monthly backup) set provides a retention period of one year. In the event that a restore is required, the data owner may request a restore of data from the backup system at any point in time, either from the daily backup-to-disk file or from the weekly/monthly backup tapes. Such a request is to be provided in writing and addressed to the AFM CIS Section.

The NAO observed that the backup software is configured to alert the IT Section CIS System Administrator. Thus, on successful backup completion or failure, an e-mail notification is sent on to the AFM CIS Section generic e-mail account. In the event that a scheduled backup fails, the IT Section CIS System Administrator must establish the root cause of failure and decide whether a manual backup should be taken. Should a backup fail to complete on two consecutive nights, a manual hot backup is performed immediately. The recording of successful backups or failures are logged on the daily and weekly maintenance checklists and the Headquarters AFM CIS Section is informed immediately whenever backups fail to complete.

As mentioned earlier, all backup media are securely stored off-site in a safe, which is only accessed by the AFM CIS Section Staff Officers. For accountability purposes, the IT Section CIS System Administrators have to sign their names whenever a backup tape is issued or returned from safe. The NAO observed that even though the backup tapes are labelled according to the *"grandfather-father"* media rotation scheme, the NAO recommends that the backup tapes should also include on every label to determine the backup media's life cycle. Furthermore, the NAO recommends that the AFM should ensure that the media is handled properly and stored in a clean controlled environment away from high temperatures, high humidity levels and the presence of dust and corrosive elements.

If all the above precautions are taken into consideration, this will increase the life expectancy of the backup media and provide assurance that data can be retrieved in the event that a file or system restore is required. In this regard, the NAO observed that every quarter the IT Section CIS System

Administrator performs test restores, according to the AFM policy *"Governing the AFM CIS Business Continuity Aspect for Servers and Application Systems"*, to ensure the proper functioning of the backup processes. Every test restore must contain records related to mission critical data and must include at least a file or folder from each backup process stored on tape or to-disk.

4.2 Identity and Access Management

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

4.2.1 Authentication

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

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

The NAO is pleased to note that the AFM CIS Section had issued a *"User Account Management Security Policy"* based on the GMICT policy, with the aim to establish the rules for the creation, monitoring, control and removal of user accounts to ensure an appropriate level of protection for Information Systems and resources in use within the AFM.

During the course of this IT Audit, the NAO observed that all the requests for the creation, modification and deletion of user accounts to access any of the AFM CIS resources, must originate from the respective Headquarters AFM Branches, Sections or Regimental Headquarters on behalf of the users under their command. These requests must then be addressed to the appropriate Information Asset Owner who must authorise the request based on a legitimate business need. Thus, for instance the Information Asset Owner for the AFM HRMIS is designated to the AFM Personnel and Administration Branch, whilst the Finance Management Section is responsible for DAS.

Furthermore, the NAO observed that the Headquarters AFM CIS Section liaises with MITA, through the electronic Request for Service (eRFS) Portal, for the creation, modification or deletion of Government e-mail, Internet and Corporate system accounts in use within the AFM, such as DAS, and FMS. Upon AFM approval, all requests have to be approved by the Ministry's IMU. The user account and password will be sent electronically by the MITA Service Call Centre on to the AFM CIS generic e-mail account. In return, the AFM CIS Section will then forward the login and password to the respective user. Similiarly, the AFM CIS Section manages all the remaining user account pertaining to the Information Systems hosted by the AFM, namely the AFM AD services, the AFM HRMIS, the DMS, the VTMIS and EUROSUR.

Meanwhile, all user accounts are immediately suspended whenever a person retires, is discharged or posted to a different section and a list of AFM officials who resigned/retired was provided to the NAO. During an on-site audit, the NAO verified that these user accounts no longer exist. In return, the Information Asset Owner and the AFM CIS Section are informed accordingly whenever there is a status change in an official's military rank.

During the course of this IT Audit, the NAO observed that the AFM CIS Section has different administrative access levels. In this regard, every technician within the IT Section CIS has a domain-admin privilege account to provide assistance and install software on end-user workstations. On the other hand, the IT Section CIS System Administrators have a system administrator account, which has elevated privileges to the current domain-admin privilege account. Rather then using the local administrator account, the system administrator account is used instead. The NAO noted that the local administrator account is hardly ever used and the administrator account password is stored in a sealed envelope and is securely kept in safe.

The NAO is pleased to note that the AFM CIS Section developed an in-house database to cater for the management of all the user accounts in use across the AFM. This database has a Microsoft Access front-end with a MySQL Back-end. The NAO observed that access to this database is restricted, whereby only the IT Section CIS System Administrator can add/modify fields and maintain the MySQL Back-end, whilst an official within the IT Section CIS has been assigned with the overall inputting and updating of data into the system. Thus, at a glance the system provides a quick overview whether a particular user has been granted access to e-mail, Internet, DAS or to any other AFM CIS resources. This database is continuously being updated to ensure that the AFM CIS Section is in control of the management of all user accounts.

4.2.2 Password Management

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

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

To enhance the level of security, the NAO observed that the *"User Account Management Security Policy"*, issued by the AFM CIS Section, stipulates a number of security controls related to password management.

All new accounts or accounts for which a password has been reset is set to expire at the next logon attempt. Once a new password is created, it is valid for a number of days before the user is prompted to change password.

A minimum password length policy has been defined so that users cannot make use of blank passwords, and users must create passwords with a minimum of eight characters in length. Furthermore, the

password must meet the complexity requirements policy setting. The policy checks all new passwords to ensure that they meet basic strong password requirements, which include a mix of letters, numbers and symbols.

Moreover, the password history has been enforced in conjunction with the minimum password age policy setting adopted by MITA to ensure that old passwords are not continually reused. In this regard, the policy has been set on all AFM domain accounts to a minimum of five passwords before an old password can be reused.

All account passwords can be easily changed by the user prior to expiration. However, if a user has forgotten his/her password, the end-user must contact the MITA Service Call Centre, to reset a password for Government Corporate systems, such as e-mail, Internet, DAS or FMS. In return, the MITA Service Call Centre will generate a new password and send the new password electronically to the AFM CIS Section generic e-mail account. The AFM CIS Section will then forward the new password to the respective user. On the other hand, the end-user must contact the IT Section CIS directly to reset their AFM Domain account or AFM owned CIS resources, such as the Document Registry System. The IT Section CIS will then generate a new password and forward it to the user over the phone or via e-mail. On the contrary and as highlighted in the previous chapter, since the EUROSUR application does not prompt the user to change their password upon first logon, the user must change their password from the EUROSUR management console. In other words, whenever the user raises a password change request, the IT Section CIS System Administrator has to logon to the EUROSUR management console and the user must physically change their password.

As mentioned earlier, the administrator account is hardly used by the AFM CIS Section and the password is kept in a sealed envelope in a secure safe. The NAO recommends that even though the administrator account password is changed upon use, the AFM CIS Section should define a procedure whereby the administrator account password be changed periodically. Furthermore, the AFM CIS Section should keep track of all password changes, the date when the administrator password was changed and the old passwords should remain accessible and stored securely, in the event that they are needed to recover a backup copy of a system.

4.2.3 Information Access Control

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

In this regard, the NAO is pleased to note that in conjunction with the previous *"User Account Management Policy"*, the AFM CIS Section issued an *"AFM File Server – Acceptable Use Policy"*. The aim is to explain the procedure to be adopted on how to provide access rights and permissions of users to access content from server and how to save the content therein.

Thus, to be able to access the AFM Servers, on a need-to-have-access basis, authorised users are granted the required privileges necessary to fulfil their responsibilities, as per least privilege principle[6]. As mentioned earlier, the same procedure applies whenever a user is granted access to a particular file.

During the course of this IT Audit, the NAO observed that the AFM CIS Section maintains all user file permissions in a centralised excel sheet. The latter keeps track of all the folder and sub-folder structure residing on the AFM servers together with a detailed description of all the user privileges assigned to every folder and subfolder. Thus, whenever a new folder/sub-folder is created or user access rights granted on a particular folder/sub-folder, the AFM CIS Section would immediately update this centralised excel sheet. The NAO commends the AFM CIS Section's initiative in maintaining a "healthy" folder structure whereby all the changes applied are recorded centrally.

The NAO also observed that the AFM CIS Section applied Disk Quotas on the AFM Servers to limit the amount of disk space that every user can use. At a glance, the AFM CIS Systems administrator will know whether users are nearing or have exceeded their assigned limit. If a user exceeds the allocated disk space and requires further disk space on server, the user has to provide a business case that must be approved by his/her superior within the AFM Branch, Section or Unit.

Apart from Disk Quotas, the AFM CIS Section has also configured a file screening management application on the AFM Servers. The aim is to prevent users from storing any non-work related files, such as audio or video files on their personal folders or shared folders hosted on the AFM Servers. In this regard, the NAO recommends that the AFM CIS Section schedules a reporting task containing a file screening audit report to monitor screening activity and storage reports periodically by e-mail.

4.2.4 Auditing

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

The NAO observed that apart from the AFM Servers, only the AFM HRMIS has audit trails in place and that access to view or modify these audit logs is restricted. Whilst reviewing the audit logs, the NAO noted that the AFM HRMIS creates an audit record every time a user accesses, creates, updates or deletes information from the system. These audit logs uniquely identifies the user, function performed and the date and time the function was implemented. Similiarly, the audit logs on the AFM Servers 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 System Administrators to detect and investigate attempted and successful unauthorised activity and to troubleshoot problems.

As highlighted in the previous Chapter, the other systems selected in the audit report, namely the VTMIS, the ICS, EUROSUR and the Coastal Radio Station do not have any audit trails because the audit functionality was not catered for when the system was developed.

[6] http://www.sans.org/reading-room/whitepapers/bestprac/implementing-privilege-enterprise-1188

4.3 Security Awareness and Training

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

In 2013, selected personnel working at the Headquarters AFM International Affairs Branch followed an *"Information Security Awareness"* course at the Centre for Development, Research and Training (CDRT) in Floriana. The objective of this course is to raise the awareness among the participants regarding the pitfalls that could be encountered when handling information. Nowadays, most of the information is in electronic format, which is retained on computers that are networked to facilitate access. This means that the need to keep the information safe and secure is even more important. The course covered real-life cases on information security incidents and various other topics that included amongst others malware, password use, surfing the net, e-mail use, protection of data, social engineering and networking, mobile devices, Wi-Fi, physical security and incident management.

The NAO recommends that other AFM officials from different Sections or Branches should attend these short training sessions on *"Information Security Awareness"* that are being offered from time-to-time by the CDRT. Since it is not possible to provide similar training sessions to all AFM officials, the NAO suggests that the AFM should draft a set of "Information Security Awareness" guidelines and disseminate them via e-mail or upload them on the AFM's Intranet with the aim:

- To inform the end-users how to protect their workstations and their personal information through the use of backups of important files and folders;

- To inform the end-users about the security risks of the Internet and highlight the appropriate actions that should be taken to minimise those risks;

- To provide 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

- To provide tips on how to safeguard your password.

The NAO recommends that these *"Information Security Awareness"* guidelines should be ongoing whereby AFM officials are provided regular updates to foster security awareness and compliance with security policies and procedures. Furthermore, these guidelines should also be provided to the AFM new recruits during their induction/military training.

In the meantime, the Headquarters AFM Capability and Training Branch is responsible for the co-ordination of the AFM's local and overseas training and education programs, including exercise planning and execution. In this regard, whenever the need arises for some AFM officials to attend

specialised training on Office Automation, the Headquarters AFM Training and Capabilities Branch will liaise with the CDRT to organise these courses hand-in-hand with the military syllabus requirement. Furthermore, the AFM Operators are offered specialised VTMIS training courses at the Malta College of Arts, Science and Technology (MCAST) or else sent on overseas training.

In this regard, the NAO observed that the AFM adopts the *"train-the-trainer"* approach, whereby the AFM officials who are sent overseas for specialised training, will then disseminate the information and offer hands-on training to the AFM officials within their Section or Unit. Furthermore, all the training material provided during the specialised courses, is easily available for reference purposes.

4.4 Anti-Virus Software

To effectively control and prevent the spread of malware, any department should adopt a reliable Anti-Virus software across its network infrastructure. The NAO observed that the AFM Servers and the PCs and laptops procured through the PC leasing scheme, are installed with the Anti-Virus software application currently being used within Government departments.

The Anti-virus application is updated automatically by MITA. Even though MITA manages all the endpoints and provides all the necessary support, maintenance and updates, the NAO recommends that the AFM request a periodic report from MITA, to ensure that all the AFM Servers, PCs and laptops are being updated with the latest definitions. Since the IT Section CIS offers first line of support on all the AFM PCs and laptops, there may be instances whereby a computer is disconnected from the network or the Anti-Virus is not functioning properly and the updates are not installed on a particular PC or laptop. In this regard, the AFM should periodically check that this is not happening.

Furthermore, the NAO recommends that the AFM requests a quarterly report from MITA that would indicate which computers were infected with malware and if the malware was removed. This report would help the AFM identify and take any necessary actions needed in the event that the same PCs or laptops are continuously being infected by malware. In this regard, the AFM should educate the users and take the necessary measures to prevent similar instances, as this might pose a risk to the AFM's network infrastructure.

4.5 Patch Management

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

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

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

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

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

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

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

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

Similiarly, the AFM Servers are also configured to download and install product updates through WSUS. However, the NAO observed that the AFM adopts a different approach on how these product updates are installed on servers. Prior to installing a product update/s, the AFM ensures that the server was backed up successfully according to the server backup schedule. Once a product update/s is installed, the server is then rebooted manually. On boot up, the AFM will ensure that no performance issues were encountered and the product update/s did not conflict with any Windows service running on servers. The remaining servers will then follow the same path.

Chapter 5

IT Operations

Chapter 5

IT Operations

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

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

5.1 Security Controls

During the course of this IT Audit, the NAO examined whether physical access and environmental controls are in place to safeguard the servers and networking equipment located at the AFM Headquarters in Luqa.

5.1.1 Physical Access Controls

Physical access controls are designed to protect the computer hardware, software and network equipment from damage, theft and unauthorised access. Therefore, restricting physical access is just as critical as restricting logical access.

To date, the AFM has two Data Rooms and two Communication Rooms located at Luqa Barracks. The NAO observed that the VTMIS servers and networking infrastructure are located in one of the AFM Data Rooms, whilst the AFM Back-end ICT services, which include the AFM AD Servers, the AFM Backup Server, the AFM Application Server and the AFM networking infrastructure, including the network connectivity to MAGNET, are located in a different Data Room. On the other hand, the ICS active equipment, the AFM ancillary networking equipment and the MCL Back-end active equipment are located in one of the AFM Communication Rooms, whilst the EUROSUR node cabinet, the Luqa Barracks fibre-optic demarcation point and the Luqa Barracks PABX telephony Back-end are located in the other AFM Communication Room.

During the course of this IT Audit, the NAO reviewed the physical access controls that are being adopted within the AFM and whether access is restricted to those who need to maintain the servers, the networking infrastructure and other ancillary equipment installed in the respective AFM Data and Communication rooms. In this regard, the NAO noted with satisfaction that the AFM CIS Section had issued an internal policy, entitled *"Access Policy and Procedures to the AFM Information System Facilities"*, which describes the physical access control security requirements and the authorisation process by which the AFM personnel may obtain access to the AFM's informational system facilities. The latter provide specific environmental enhanced security access, fire alarms, UPS, network backbone connectivity and a number of other elements required by the AFM mission-critical resources.

The NAO noted that access to the AFM Data Room hosting the AFM Back-end ICT services is controlled by means of a dual-factor authentication control system, which entails a proximity card reader and a fingerprint scanner. On the other hand, the AFM Data Room hosting the VTMIS servers and network infrastructure and the remaining AFM Communication Rooms are accessed by means of physical keys, which are located at the AFM Operations Room. The keys are handed in to authorised AFM personnel who sign in on two different logbooks whenever the keys are issued and returned to the AFM Operations Room. Furthermore, whenever the keys are issued and returned to the Operations Room, the AFM CIS Officer in charge or his delegate must sign in/out during office hours, whilst the AFM Duty Officer must sign in/out during silent hours.

In the event that the proximity card granting access to the AFM Data Room highlighted above is lost, stolen, misplaced or damaged, the owner of the card must immediately inform the CIS Staff Officer or his representative and the Force Security Officer. In this regard, the card is immediately blocked and a new one is issued. Similarly, if an AFM authorised user loses a key of any of the above Communication Rooms or Data Room, he/she must immediately inform the AFM CIS Section Commanding Officer and the Force Security Officer who will ensure that the locks are changed as soon as possible.

The NAO observed that the AFM CIS Section Staff Officer is authorised to process individual requests for AFM personnel to be provided access to the AFM Data and Communication Rooms. Furthermore, the AFM Data Room where the AFM Back-end ICT services are located has two different access levels:

- **Controlling Access** – this is granted to AFM personnel to have free access to enter the AFM Data Room in line with their job responsibilities that require them to have access. In this regard, only the AFM personnel with controlling access are provided with an access proximity card for entry in the AFM Data Room;

- **Escorted Access** – this level of access is closely monitored, whereby access is granted to AFM personnel or third party suppliers who have a legitimate business need to enter the AFM Data Room. The AFM personnel with escorted access are not provided with an access proximity card and will be requested to sign in and out on the AFM Access Control Registry Book under the direct supervision of AFM personnel with controlling access, and must leave the premises when requested to do so.

In the meantime, the other AFM Data Room and the two Communication Rooms have similar access levels. However, personnel with escorted access level or visitors are not obliged to sign in and out on

the AFM Access Control Registry Book when entering any of the two Communication Rooms or the Data Room where the VTMIS is located. However, each time an individual with escorted access or visitor is admitted to the AFM Luqa Barracks, the individual must sign on a different Access Control Log at the time of entrance. A visitor's tag is handed to the individual and must be visibly worn at all times. Before leaving, the individual must return the visitor's tag and sign the time of exit.

The NAO notes with satisfaction that quarterly reviews are carried out by the AFM CIS Section of all individuals with any levels of access to the AFM Data and Communication Rooms. Access is revoked if an individual no longer requires access to the AFM Data Room. In this regard, the procedures for terminating or revoking access include the cancellation of the access proximity card, deletion of the individual's name from the AFM's Operations Authorised Access List and the deletion of the fingerprint profile linked to the individual from the access control database.

Burglar alarms and surveillance systems mitigate the risk of undetected physical intrusion by serving as a detective control as well as a deterrent for would-be intruders. The absence of these controls increases the risk of theft and other criminal activities. However, this risk is mitigated by the fact that the AFM has armed guards on a 24/7 roster, who carry out a number of patrols around the AFM premises and barracks.

5.1.2 Environmental Access Controls

Environmental exposures should be given the same level of protection as the physical exposures. Environmental exposures are due primarily to naturally occurring events such as lightning, flooding, fire, electrical interruption and other environmental disasters. During the course of this IT Audit, the NAO examined whether the AFM Data and Communication Rooms have any environmental controls in place and what measures are being taken to mitigate the related risks.

The NAO noted that none of the AFM Data and Communication Rooms has a fire suppression system in place. On the other hand, only the AFM Data Room, hosting the AFM Back-end ICT services, is equipped with smoke detectors. The latter are connected to a central fire alarm system, which is powered by the main electrical distribution and backed up with battery power. If smoke is detected inside the room, it will produce an audible alarm when activated. Smoke detectors are inspected and tested annually by a local supplier.

Furthermore, the NAO observed that only the AFM Data Room hosting the AFM Back-end ICT Services is equipped with fire extinguishers. However, a number of fire extinguishers are installed in strategic locations and offices within the Headquarters AFM in Luqa. These are inspected and serviced once a year by a local supplier.

The NAO observed that all the AFM Data and Communication Rooms are equipped with two air conditioning units, one of which is kept on at all times. In the event of a hardware malfunction, the second air conditioning unit is switched on instead. In the meantime, the temperature and humidity levels inside the AFM Data room, hosting the VTMIS equipment, are being monitored daily by the IT Section CIS System Administrators. During the on-site IT Audit visit, the NAO noted that the AFM Data Room, hosting the AFM Back-end ICT services, did not have a temperature and humidity monitor in

place. However, the NAO was informed that the AFM CIS Section procured a mobile temperature and humidity monitor. The latter is currently being kept inside the AFM Data Room, to ensure that the temperature and humidity levels are adequate.

In the event of a power failure, all the AFM servers, networking equipment and other ancillary equipment are connected to a UPS. The latter will safeguard all the IT components connected to them from any power surges or unexpected shutdown. Since the AFM servers have dual power supplies, these are installed on to different UPSs. Thus, in the event of a hardware malfunction on one of the UPSs, the AFM servers will remain switched on, as the load will be shifted on the remaining UPS.

The NAO also noted that in order to maintain the security and smooth operation of the Back-end active equipment and the networking equipment hosted at the respective Data and Communication Rooms, the AFM adhere to the internal *"Access Policy and Procedures to the AFM Information System Facilities"*, which stipulates that:

- No food, drink and smoking is allowed inside any of the AFM's Information System facilities;
- Any goods intended for the AFM Data Room are to be packed and unpacked outside the room and thus no packaging material is allowed inside the rooms;
- Photography and filming is not allowed inside the AFM premises.

The NAO noted that even though the AFM Data and Communication Rooms do not enjoy the standard facilities which modern Data Centres are equipped with, the NAO took into consideration the AFM IT Strategy *"The AFM CIS Migration towards a Federated Environment"* highlighted earlier in the report. This IT strategy envisages that a new Data Centre will consolidate all the AFM CIS services, applications, networking and communications infrastructure, to ensure the availability, performance and reliability of the AFM CIS services in support of military operations and administrative functions. Upon request, MITA provided the AFM with a high-level configuration setup, including a budgetary estimate for the proposed data centre facility, which would include:

- Two modular Computer Rooms for the hosting of servers and telecommunications equipment, a power room, a UPS room, a staging/storage area and an office area;
- Fire compartmentation between each room;
- Four independent automatic fire suppression system based on CO_2 and Argonite;
- A robust power supply based on two distribution circuits and backed by the in-house generator;
- A UPS plant room;
- Rack mounted UPSs to provide the second independent power supply;
- Closed control air-conditioning to control temperature and humidity levels;

- Access control system;
- CCTV system;
- Raised flooring system to provide under flooring cooling plenum and power cable management; and
- Flexible data cabling system based on fibre-optic and UTP.

5.2 IT Service Management

The IT Service Management (ITSM) practices are important to provide assurance to the AFM end-users and high-ranking officials that the expected level of service is being delivered.

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

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

As highlighted in the previous chapters of the report, the IT Section CIS offers first line support to all AFM end-users, whereby all the end-users must submit all their requests for hardware and software assistance to the IT Section CIS by e-mail, phone or in person. If the problem could not be resolved over the phone or on-site, due to a hardware malfunction, the IT Section CIS will raise a service request with MITA's Service Call Centre. In this regard, a reference number is generated from MITA's Call Logging System whereby a notification is automatically sent by e-mail to the IT Section CIS generic e-mail account. The NAO noted that the IT Section CIS saves the e-mail notification offline whilst a hard copy is printed and stored in a file. When the third party supplier calls on site, the third party supplier's job sheet is then attached to the hard copy of the e-mail notification. The same procedure applies whenever a third party supplier is called upon to service an AFM owned IT application or servers.

Even though the IT Section CIS keeps track of all the incidents that are escalated to the respective third party suppliers in a file, the NAO noted that the IT Section CIS does not keep track of any incoming internal IT service requests. In this regard, the IT Section CIS cannot quantify the amount of calls that are being handled on a daily basis, whether there are any recurring problems on the same hardware equipment or software application to correlate identical incidents. This data could be used to justify a hardware replacement or solve the root cause of the problem. Thus, the NAO recommends that all the incidents be recorded electronically in a call logging system or in a simple centralised spreadsheet. In this regard, the IT Section CIS could then easily trace when a problem was first encountered, whether repetitive calls were made and when the problem was solved. Furthermore, the amount of calls registered would substantiate the level of support being provided by the IT Section CIS across the AFM and would even help in human resources capacity planning and decision-making.

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

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

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

Finally, since most of the IT applications included in this IT Audit report are EU Funded, the onus of change management is on the respective third party supplier. A sound change management includes formalising and documenting the process of a change request, obtain a written authorisation, carry out the necessary testing, implement the change request and finally communicate to the respective users when the change is completed. In this regard, whenever a system or software upgrade/hotfix is required, the respective third party supplier will liaise with the AFM CIS Section as stipulated in the signed SLAs between the AFM and the third party supplier.

5.3 E-mail and Internet Services

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

The AFM's e-mail and Internet services are being provided by MITA through the Government's communications backbone, MAGNET. In this regard, the NAO noted that the AFM CIS Section had issued an *"AFM Electronic Mail Acceptable Use Policy"* in line with the e-mail and Internet services policy and directive[7] that were issued by the former Central Information Management Unit (CIMU) in 2003.

The NAO observed that almost every AFM official was provided with an e-mail and Internet account. The AFM policy highlighted above stipulates that the e-mail service is provided for business use only and is deemed the property of AFM. Any e-mail, including attachments, that are created, sent, received or printed via the e-mail service, becomes the property of the AFM. Furthermore, the personal use of e-mail is allowed only in exceptional cases and provided that this does not interfere with the performance of the account holder's duties or those of other account holders.

[7] https://www.mita.gov.mt/page.aspx?pageid=220

On a similar note, every user is responsible and held accountable for Internet activities done. Thus, all the AFM officials who own an Internet account must also abide by the AFM internal policy *"Acceptable Use Policy for the AFM Communications and Information Systems Resources"*. Even though an adequate filtering technology is being used by MITA, to prevent access to illegal material, every user should ensure that his/her account remains secure and should not disclose the password or use someone else's password.

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

In the meantime, the NAO noted that all e-mail and Internet accounts created, modified or deleted must have a documented request initiated by the respective Headquarters AFM Branches, Sections or Regimental Headquarters for authorisation on behalf of the end-user. These requests are then forwarded to the Headquarters AFM CIS Section according to the AFM *"User Account Management Security Policy"*. In return, the Headquarters AFM CIS Section will then forward the necessary requests to MITA through the eRFS Online Module.

The NAO recommends that the Headquarters AFM CIS Section should periodically remind all the AFM officials who own an e-mail or Internet account, about the salient points highlighted in the AFM Internal policies mentioned above especially the restrictions on use of e-mail and Internet services as reproduced in Appendix D.

5.4 Web Filtering

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

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

The web filtering can be configured to either *"whitelist"* or *"blacklist"* a website. Websites found in the "whitelist" group can only be accessed when *"whitelist"* is enabled. On the other hand, if *"blacklist"* is enabled, the web filter will allow all websites except those listed in the *"blacklist"*. In the event that

a particular website is being blocked or needs to be blocked by the web filter, the Headquarters AFM Branches, Sections and Units report the web site in question to the AFM CIS Section. In return, the Headquarters AFM CIS Section will liaise with MITA's Service Call Centre to take the necessary action to *"whitelist"* or *"blacklist"* the web site accordingly.

5.5 AFM Internal and External Communications

Communication can take various forms but all forms involve the transfer of information from one party to another. Just like any organisation, the AFM strives to be proactive in both its operations and even where military media relations are concerned. In 2010, the AFM decided to create a new AFM Website whilst an official Facebook page was launched in 2012, followed by the creation of the AFM YouTube Channel in 2013.

The AFM Website, the official Facebook Page and YouTube Channel are online platforms at the disposal of the Command structures of the AFM. These platforms are means to communicate efficiently and effectively with members of the public to project a highly versatile and professional force that is of service to the Republic of Malta and its' citizens. Furthermore, the objective of these online platforms is to get more young people interested in joining the force and to promote the AFM as an organisation that is an equality employer as well as a main contributor towards the wellbeing of the Maltese society. Moreover, the AFM Intranet is solely being used internally by the AFM personnel as a key communication tool to provide timely and accurate information.

During the course of this IT Audit, the NAO observed that in terms of the AFM internal and external communications, apart from the *"E-mail Acceptable Use Policy"* and the *"Acceptable Use Policy for AFM CIS Resources"* highlighter earlier, three internal policies were issued by the AFM namely:

- *"AFM Online Authoring and Publishing Policy"*;
- *"AFM Website and Social Media Management Policy"*; and
- *"AFM Intranet Policy"*.

In this regard, the NAO looked into how the AFM is managing its own internal and communication tools, namely the AFM Website, the official Facebook page, the YouTube Channel and the AFM Intranet website.

5.5.1 AFM PI Cell

The AFM PI Cell falls within the remit of the Headquarters AFM Administration and Personnel Branch under the command of one commissioned AFM Staff Officer III, serving as the official Public Relations officer of the AFM. Apart from the Staff Officer, the AFM PI Cell is made up of four personnel, which include:

- a Staff Sergeant serving as an Assistant to the AFM PI Cell commanding officer;
- a Bombardier as the official AFM Photographer;
- a Gunner serving as a Graphic Designer and Video/Photo editor; and
- a Gunner serving as an Editor responsible for the overall uploading of information on the AFM internal and communication tools.

Whilst the AFM PI Cell is tasked to advise the Commander AFM on matters relating to public information, the overall mission tasking of the AFM PI Cell is to ensure that the AFM media operations' activities are timely and accurate. Furthermore, the AFM PI Cell, through its Defence Media Operations, aims to create and maintain a favourable public image of the Maltese military, and continue to foster support and interest by the public in the AFM, its personnel and operations. This is achieved by promoting widespread public understanding and support for military operations, whilst maintaining operational security and countering the dissemination of hostile and potentially damaging information.

In this regard, the *"AFM Online Authoring and Publishing Policy"* stipulates that the AFM Staff Officer III, responsible for the AFM PI Cell, acts as the release authority for all the AFM online content and is primarily responsible to ensure that all published material accurately presents the AFM with a high level of professionalism with the aim to:

- Make all reasonable efforts to verify the accuracy, consistency, appropriateness and timeliness of all AFM online content;
- Review all the information, graphics and photos for all the levels of security and other concerns before it is released;
- Ensure that the AFM online content is appropriate for worldwide dissemination and does not place national security, AFM personnel and assets, mission effectiveness or the privacy of individuals in an unacceptable level of risk; and
- Acts as the filter point and the one to follow up any enquiries received through the website, which is to be handled in a similar way to other written requests for information.

The NAO observed that the AFM PI Cell handles a considerable amount of photographic images and audio/video files, which are being backed up on CD's and DVD's. Moreover, the AFM PI Cell has an external 1.5TB hard drive, which is being used to backup High Definition (HD) video footage especially when dealing with video production entities in joint productions. However, since the HD video footage takes a lot of Hard Disk space, sometimes the AFM PI Cell are finding it difficult to backup all the data on the external hard drive. In this regard, the NAO recommends that the AFM PI Cell together with the AFM CIS Section should come up with a solution to provide a Media Server, whereby all the digital media (digital videos/movies, audio/music and photo images) can be stored online and easily accessed over the network.

Finally, the NAO noted that with its' limited resources, the AFM PI Cell goes to great lengths to update all the AFM online platforms on a 24/7 basis to serve as an information hub to the journalists and to the public. In this regard, news headlines referring to the AFM operations can now be accessed on a PC, TV, Tablet or Smartphone, as a result of the level of support that the AFM PI Cell are being offered by the various AFM Sections and Branches.

5.5.2 AFM Website

The implementation of the new AFM website is accessible through the following Uniform Resource Locator (URL) http://www.afm.gov.mt in compliance with the Government's *"Website Content and Presentation Standard"* GMICT S 0051-1:2012[8].

The AFM website is an updated platform highlighting all the aspects of the Maltese military. It provides a detailed description of the Force today that is organised, trained and equipped to conduct military operations at a national level as well as to contribute towards international crisis management. It also provides information on weapons, military history, uniforms or equipment in use within the AFM.

During the course of this IT Audit, the NAO reviewed the AFM website and how the AFM PI Cell is maintaining the website content. In this regard, the NAO was informed that the AFM website is being hosted and backed up by MITA, whilst the Back-end is being provided by a local third party supplier. Thus, there are two main Back-end platforms to cater for the AFM website. The first Back-end platform is known as the OPM Central, whereby the AFM PI Cell has access to edit the "NEWS", "EVENTS" and "VIDEO" content found primarily on the AFM Homepage. The second Back-end platform, known as the AFM Publisher, controls all the other pages of the website. The AFM PI Cell accesses the AFM Publisher to change the content and aesthetics of the AFM website when required.

The NAO also noted that users, who are not particularly attracted to militia, could utilise the AFM website to access free fitness programmes or the nutrition section containing advice on how to stay fit and healthy. Through the AFM Homepage, users can also access the AFM official Facebook page and the AFM YouTube channel.

[8] https://www.mita.gov.mt/page.aspx?pageid=220

The NAO observed that the AFM PI Cell, publishes the annual *On Parade* magazine, which is distributed free of charge together with a local newspaper. A soft copy can be downloaded from the AFM website under the Info Centre heading. When compared to the previous editions, the NAO noted that the articles found on this year's *On Parade* magazine could be downloaded more easily. Rather than splitting an article into different downloads, according to the number of pages, the article can be downloaded into one file.

5.5.3 AFM Facebook Page

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

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

The AFM has recognised the potential of social media as a modern communication channel and in this regard, the AFM PI Cell launched the official AFM Facebook page. To date, the AFM Facebook page has grown exponentially, since it was launched in 2012, with over 4,000 likes and an average reach of 15,000 users a week.

The AFM Facebook is serving as a showcase medium for all public relations initiatives and is the culmination of a professional and co-ordinated effort that highlight the work of those men and women that serve our nation. In this regard, the AFM Facebook timeline exhibits a wide array of articles. These vary from AFM rescue operations to official state visits by foreign dignitaries and AFM ceremonial engagements.

5.5.4 AFM YouTube Channel

YouTube is a video-sharing website whereby users can upload, share, comment on and view videos. In this regard, the NAO observed that in 2013, the AFM PI Cell launched the AFM's YouTube Channel to reflect all the AFM's corporate identity. The AFM YouTube Channel can be viewed either directly from the main YouTube website or from the YouTube link found on the AFM Homepage. Furthermore, it is also embedded in the AFM Facebook page to improve interlinking and marketing reach. To date, the AFM YouTube channel has over 60,000 views.

The AFM YouTube Channel is an ideal way to upload official in-house productions to display operations and happenings within the force. It also serves as a data bank that is used for the media in their quest for operational footage. In this regard, links from this channel are widely used both internally and externally with local or foreign media, whereby the description of all the AFM YouTube videos is

official and a carbon copy of the sanctioned press release. Furthermore, all the footage that features the AFM in local TV stations is collected, converted and uploaded on the AFM YouTube Channel.

5.5.5 AFM Intranet

During the course of this IT Audit, the NAO observed that the AFM CIS Section is responsible for the overall direction, management and strategy of the AFM Intranet. In this regard, the AFM CIS Section drafted an AFM Intranet Policy to establish guidelines and assign responsibilities for anyone authoring, publishing or administering web content on the Intranet.

The AFM Intranet is an internal website that was commissioned by the CIS Office in February 2011. It was designed in-house by a non-commissioned Officer responsible for the IT Section CIS, for the exclusive use and benefit of AFM personnel as a key communication tool to provide timely and accurate information.

The AFM Intranet is published for AFM personnel to obtain the necessary information in the course of their official duties. It is accessible through the AFM network without the need for a login identification and authentication. The AFM Intranet policy applies to all AFM personnel and stipulates that *'the information given in the AFM Intranet is not to be communicated either directly or indirectly to the Press or any other person not authorised to receive it'*.

The publication and ownership of content on the Intranet is delegated to the respective Headquarters AFM Branches, Sections and Units. Thus, it is the responsibility of the AFM Branch Chiefs, Section Heads and Unit Commanding Officers to ensure that information produced on behalf of their Branch, Section or Unit and which is intended for use by personnel is approved by them before it is published on the AFM Intranet. Furthermore, they are to oversee that any owned information is accurate, timely and up-to-date and must exercise extreme caution to ensure that they do not post classified material. In this regard, the respective AFM Branch, Section or Unit appointed an official to publish information and to keep the content that is owned and published accurate and up-to-date.

The AFM CIS Section took over the responsibility for the overall direction, management and strategy of the AFM Intranet, the 4th Regiment AFM CIS Company Intranet Administrators provide technical support and maintenance, manage user permissions and address any technical issues that may arise. Furthermore, the AFM CIS Section also:

- Monitors and ensures the proper and effective use of the AFM Intranet;
- Makes decisions on where content should be placed;
- Liaises with the 'owners' of information hosted on the AFM Intranet on a regular basis, to ensure they proactively manage information which falls under their remit;
- Provides policy direction for the 4th Regiment AFM CIS Company Intranet administrators on all technical matters relating to the AFM Intranet;

- Ensures the implementation of the Intranet policy; and

- Reviews the Intranet policy and any related guidelines to ensure they work effectively to promote and support efficient and effective use of the AFM Intranet.

The NAO observed that the AFM Intranet is hosted on a virtual environment, which is installed on one of the AFM Servers. The AFM CIS Section ensures that the virtual environment is saved and backed up daily to disk on the AFM backup server.

5.6 Risk Management

During the course of this IT Audit, the NAO observed that the AFM does not have formalised IT Business Continuity and Disaster Recovery plans covering all the critical IT components within the AFM. However, a number of initiatives were taken by the AFM CIS Section to mitigate the risks involved in the event of a disruption or total failures in the IT systems within the AFM.

In this regard, the NAO suggests that the AFM should perform a Business Impact Analysis and a Risk Assessment exercise from which a Business Continuity and Disaster Recovery plans can be drafted as represented in Appendix E.

5.6.1 Business Impact Analysis

A Business Impact Analysis is a critical step in developing a Business Continuity Plan (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 detailing likely incidents and their related business impact in terms of time, resources and money. This report should give an understanding of the impact of non-availability of the IT systems and components and how will this affect the *'modus operandi'* within the AFM.

The NAO recommends that the Business Impact Analysis process is based upon the information that is collected from the high-ranking AFM officials and key persons within the AFM CIS Section. The information can be collected using different approaches. One of the popular approaches is the questionnaire approach whereby a detailed questionnaire is circulated to key users in IT and to the end-users. Another alternative is to interview groups of key users. The information gathered during these interviews or from the questionnaire response, is tabulated and analysed for developing a detailed Business Impact Analysis plan and strategy.

Furthermore, the NAO recommends that the AFM lists and reviews its critical and non-critical functions. For each critical function, the AFM should then determine:

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

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

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

5.6.2 Risk Assessment

The NAO believes that a cost-effective BCP and Disaster Recovery Plan (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 the AFM fails to identify the above-mentioned risks, it can neither plan nor manage the processes to mitigate those risks.

The NAO recommends that the AFM should carry out a risk assessment to analyse the value of their 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 types of threats that are to be analysed assigning a probability assessment value to each.

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

5.6.3 Business Continuity and Disaster Recovery Plans

The primary objective of a BCP is to protect the AFM in the event that all or parts of its operations and/or Information Systems are rendered unusable and to help the AFM 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 Risk Assessment exercise.

In terms of the AFM, a BCP is an integral concept in their day-to-day operations that falls under the remit of operational planning and staffed by the Headquarters AFM Operations, Plan and Intelligence Branch, which is then translated into plans and SOPs. In this regard, the control room at Lyster Barracks in Ħal Far can assume operational command of the AFM operations in the event that the main Operations Centre at Luqa Barracks is down. The AFM Communications and Command Vehicle can also be deployed for this purpose. Moreover, the AFM is also equipped with dual radio communications (the ICS system and the legacy communications) in the event of a service disruption.

During the course of this IT Audit, the NAO notes with satisfaction that the AFM CIS Section had drafted an internal policy on how to recover an AFM information or application system in the event of a service disruption. In this regard, the AFM Standing Orders Section 44 Part 1 General *"Policy Governing the AFM CIS Business Continuity Aspect for Servers and Application Systems"* defines the backup and restore policy being adopted to guarantee the continued provision of CIS services in support of the AFM operations and administration.

Whilst a BCP refers to the activities required to keep the AFM operations running during a period of interruption of normal operation, a DRP is the process of rebuilding the operations or infrastructure after the disaster has passed.

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

The NAO was informed that DRP plans are being drawn up by the AFM, in conjunction with MITA, and will include a data replication of the AFM servers so that CIS operations can be resumed from the MITA-01 Data Centre. Moreover, taking into consideration the importance of the AFM Operations Centre, the NAO recommends that a DRP should include documented information on how to shift operations in the event of service disruption.

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

Chapter 6

Management Comments

Chapter 6

Management Comments

The existing AFM IT strategy is currently being revised as to date, the proposed Data Centre and the upgrade of the AFM WAN have not yet materialised. Apart from solely focusing on the IT infrastructure, as it was the current strategy focus, this new study will provide a complete strategic analysis that will broaden the focus on both the AFM Business Information Systems and IT infrastructure requirements. From the findings of this analysis, the AFM will formulate a Business Renovation Strategy integrating a Continuous Process Improvement and Business Process Re-engineering to align the Information Systems and IT infrastructure strategy for successful e-business execution.

Following the recent integration of the CIS Section within the Procurement and Logistics Branch, for the first time the section was allocated a specific budget line for Information Systems and IT. This important milestone coupled with the funds available through the European Union to invest on infrastructure projects, have given the section the possibility to invest, evolve and thrive according to the current standards and requirements of today. In fact, one of the major projects underway as regards IT infrastructure in the AFM will be the AFM Microwave link network mainly financed through the European Border Fund (EBF 2013). The External Border Fund application for the upgrade of the Microwave link was submitted on 15th November and is now being processed. The AFM Microwave link network is specifically used for the purpose of border control operation systems such as VTMIS and ICS. On the other hand, with regards to the WAN, the AFM has initiated a study to explore market options on how to improve the bandwidth supply to match the bandwidth demands of its remote facilities.

On a parallel line with the above mentioned infrastructure projects, the AFM is simultaneously consulting with the original developer of the AFM HRMIS to rejuvenate this application through re-encoding from Visual Basic to JavaScript, including modification of the suggested Security Logins as per MITA password strength, password complexities and expiry.

The AFM has also recognized the need to expand the scope of its online IT Inventory. The AFM already has an online inventory, which however includes only personal computers and laptops, whilst all the

other inventories are still kept manually on paper. Following the recommendation in this audit report, the online inventory will be further developed to include other peripherals such as print servers and printers. Moreover, this online IT inventory will also be expanded to serve the purpose for the software and licensing inventory.

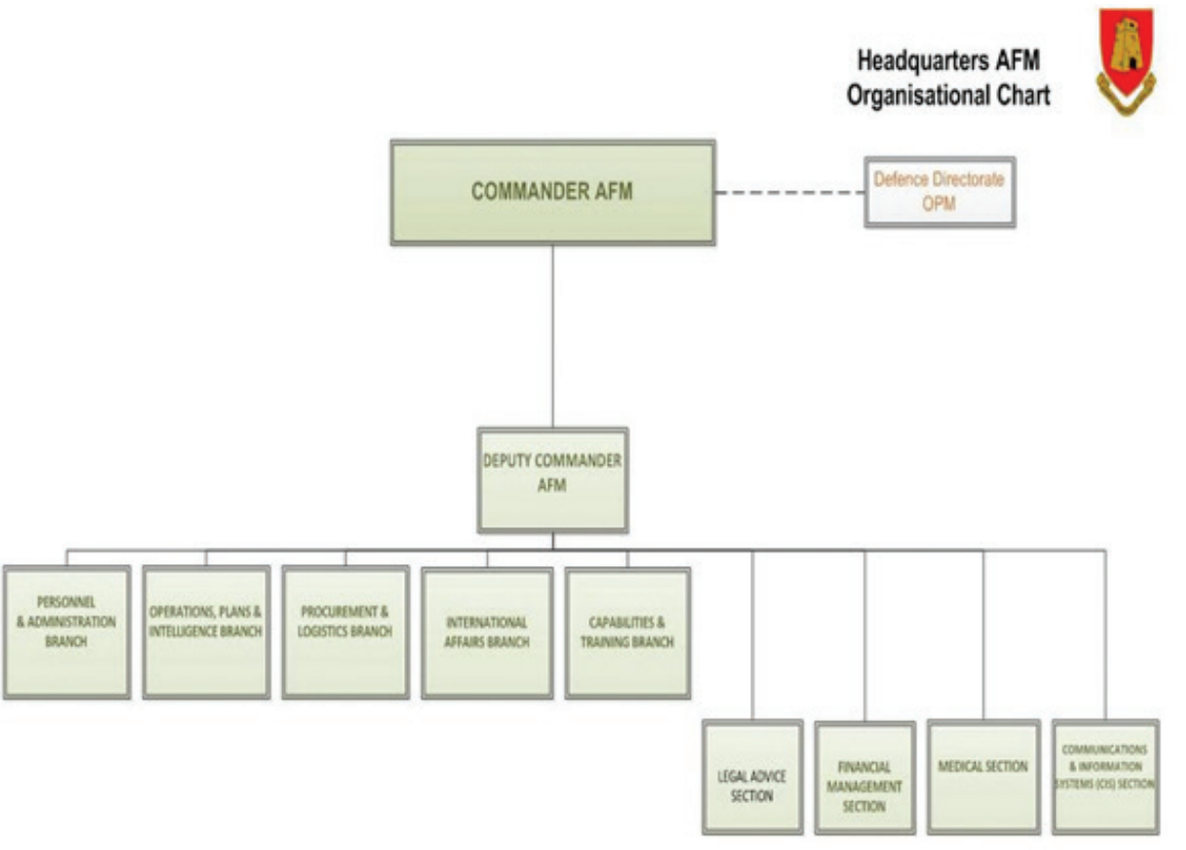
The AFM fully concurs with the recommendation in the audit report to formulise a Business Impact Analysis and will do so accordingly. The organisation fully acknowledges the need for an adequate Business Continuity and Recovery Plans. As at today, the AFM has the capability to make a full Business Recovery through the Microsoft Data Protection Manager backups. The AFM is planning to implement a Microsoft Distributed File System in two different locations. This will facilitate file replication, provide high accessibility to file sharing, minimising the network traffic on the WAN connections and provide redundancy in case of failure.

Finally, the AFM would like to thank the National Audit Office, the Auditor General and their respective auditors for their time, commitment and contribution towards this audit report.

Appendices

Appendix A

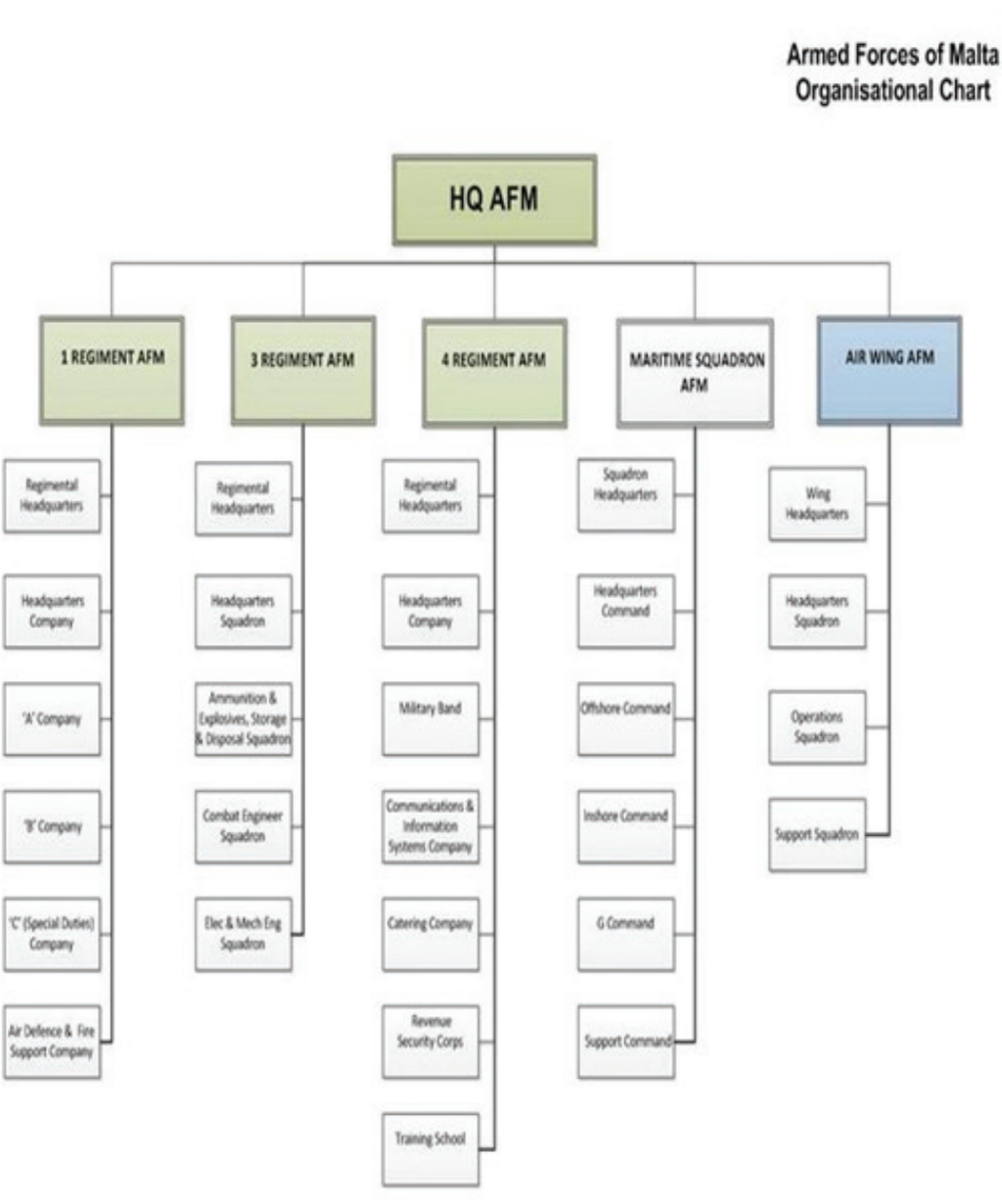
Headquarters AFM Organisation Chart[9]



[9] The Headquarters AFM Organisational Chart was provided by the AFM CIS Section in August 2013

Appendix B

AFM Organisational Chart[10]



[10] The AFM Organisational Chart was provided by the AFM CIS Section in August 2013

Appendix C

COBIT Controls

COBIT 4.1 defines IT activities in a generic process model within four domains[11]. 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.

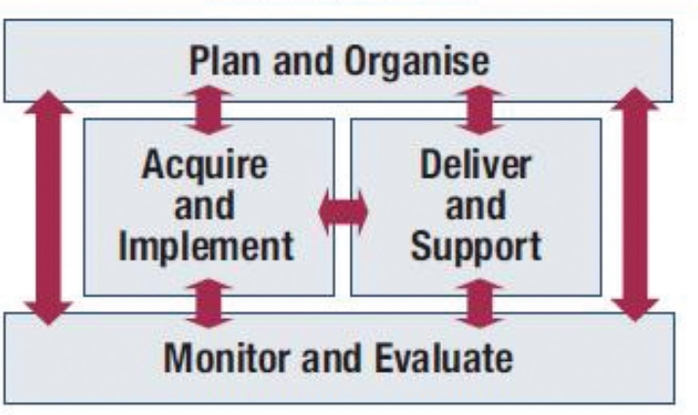


Figure 4 – COBIT Controls

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.

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

Assess and Manage IT Risks

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

Acquire and Implement Domain

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

Manage Changes

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

Install and Accredit Solutions and Changes

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

Deliver and Support Domain

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

Define and Manage Service Levels

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

Manage Third party Services

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

Ensure Continuous Service

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

Ensure Systems Security

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

Manage the Physical Environment

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

Manage Operations

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

Monitor and Evaluate Domain

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

Provide IT Governance

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

Appendix D

Restrictions on use of e-mail and Internet services

Restrictions on use of e-mail services[12]

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

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

[12] As per the AFM "Electronic Mail Acceptable Use Policy" issued by the AFM CIS Section.

Restrictions on use of Internet services[13]

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.

[13] As per the AFM "Acceptable Use Policy for the AFM Communications and Information System Resources" issued by the AFM CIS Section

Appendix E

Business Continuity and Disaster Recovery Plan[14]

A Business Continuity Plan should:

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

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

- Implement a process for periodic review of the BCP's continuing suitability as well as timely updating of the document, specifically when there are changes in technology and processes, legal or business requirements;

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

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

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

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

A Disaster Recovery Plan should contain the following information:

- A statement detailing the scope and capability of the disaster recovery plan, exactly when should this plan be used and what is the impact on the AFM;

- A description of the key roles and responsibilities so that anyone assigned to a particular role in the recovery team understand what is required of them;

- A summary of the critical services, their recovery objectives and recovery priorities;

- Third party contact details, particularly those that may be required to assist in the recovery of resources or services that are being maintained within the AFM;

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

RECENT AUDIT REPORTS ISSUED BY THE NAO

NAO Work and Activities Report

January 2013	Work and Activities of the National Audit Office 2012

NAO Audit Reports

March 2013	Performance Audit: Simplification of the Regulations in Structural Funds
April 2013	Enemalta Corporation Delimara Extension Implementation
May 2013	Performance Audit: Managing Public Service Recruitment
June 2013	Information Technology Audit: Primary and Secondary State Schools
June 2013	Performance Audit: The Management of Elective Surgery Waiting Lists
July 2013	Information Technology Audit: Institute of Tourism Studies - Malta
July 2013	Performance Audit: An Analysis of the Effectiveness of Enemalta Corporation's Fuel Procurement
September 2013	Performance Audit: Enforcement Action by MEPA within the Outside Development Zone
November 2013	An Analysis of the National Lotteries Good Causes Fund
December 2013	Performance Audit: Road Surface Repair Works on the Arterial and Distributor Road Network Follow-up
December 2013	Annual Audit Report of the Auditor General - Public Accounts 2012
January 2014	Performance Audit: Addressing Social Benefit Fraud