Information Technology Audit

Medicines Authority

Table of Contents

Figures

Tables

List of Abbreviations

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

ATC	Anatomic Therapeutic Chemical
BEMA	Benchmarking of European Medicines Agencies
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
CCTV	Closed-Circuit Television
CD	Compact Disc
CEO	Chief Executive Officer
CIMU	Central Information Management Unit
CoBit	Control Objectives for Information and related Technology
CTFG	Clinical Trials Facilitation Group
CTS	Communications and Tracking System
DVD	Digital Versatile Disc
eCTD	Electronic Common Technical Document
EiY	European Union Review System is Yours
EMA	European Medicines Agency
E-Mail	Electronic Mail
EU	European Union
EUDRA	European Union Drug Regulatory Authorities
EudraCT	European Union Drug Regulating Authorities Clinical Trials
EudraGDP	European Union Drug Regulatory Authorities Good Distribution Practice
EudraGMP	European Union Drug Regulatory Authorities Good Manufacturing Practice
EURS	European Union Review System
EUTCT	European Union Telematics Controlled Terms
EV	EudraVigiliance
EVDAS	EudraVigiliance Data Analysis System
GMICT	Government of Malta Information and Communication Technology

GMP	Good Manufacturing Practice
ICT	Information and Communication Technology
IP	Internet Protocol
IS	Information Systems
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAGNET	Malta Government Network
Mbps	Megabits per second
MDIS	Maltese Drug Information System
MITA	Malta Information Technology Agency
NAO	National Audit Office
OPM	Office of the Prime Minister
PABX	Private Automatic Branch eXchange
PC	Personal Computers
RFI	Request for Information
SEP	Symantec Endpoint Protection
SOP	Standard Operating Procedure
SPC	Summary of Product Characteristics
SQL	Standardised query language
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
VPN	Virtual Private Network
WSUS	Windows Server Update Services

Chapter 1

Overview

The Medicines Authority was established in 2003 as an autonomous body to contribute to the protection of public health in Malta and within the European Union (EU) through the regulation of the safety, quality and efficacy of medicinal products for sale or supply on the Maltese and the EU market.

Furthermore, the Authority is committed to providing high quality licensing, monitoring and inspection service for pharmaceutical activities, to enforce the relevant legislation.

The Authority is also responsible for post licensing safety monitoring through pharmacovigilance and adverse drug reaction reporting, as well as for monitoring the advertising of medicinal products.

The Medicines Authority also has a national public health remit with respect to pharmaceutical activity, information about medicinal products, and the availability and use of medicinal products on the local market.

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

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

1.1 Background

The Medicines Authority is entrusted with protecting and enhancing public health both in Malta and the EU. The Medicines Authority has its regulatory function delegated by the Licensing Authority. The Medicines Authority carries out the evaluations of applications and gives its recommendations to the Licensing Authority. Based on these evaluations and recommendations, the Licensing Authority will then authorise the products and issue licenses.

In this regard, during 2011 the Authority authorised 491 medicinal products through European and National Procedures including 11 procedures where Malta was the Reference Member State. The total amount of products authorised in Malta (excluding the centrally authorised products) as at the end of 2011, amounted to 3,947.

Furthermore, the Medicines Authority collaborates with other Medicines and Healthcare Regulatory Agencies so as to increase the inclusion of Malta as a Concerned Member State. During 2011, the Authority has collaborated with the Medicines and Healthcare Regulatory Agency (UK) and the Irish Medicines Board.

The Medicines Authority also monitors the medicinal products on the market after authorisation. During 2011, the total amount of inspections (Good Clinical Practice, Good Manufacturing Practice, Good Distribution Practice, Pharmacy and Pharmacovigilance inspections) amounted to 221.

The Medicines Authority undertakes several activities for the purpose of attaining effective product safety surveillance, amongst which are the:

- Approval of Direct Healthcare Professional Communications detailing safety/risk changes to scientific information and recommendations on product administration methods;

- Investigation of newly identified safety signals with immediate product suspension and/or recall as relevant (Safety Signal Investigations, Rapid Alerts and Product Safety Recalls);

- Approval and monitoring of Pregnancy Prevention Programmes as proposed in relation to potentially teratogenic medicinal products;

- Monitoring of risk minimisation programmes relating to high risk medicinal products and provision of the relevant regulatory information in order to establish such programmes;

- Communication as relevant with the Department of Healthcare Services Standards on toxicological risks identified in relation to blood products (Haemovigilance);

- Initiation and subsequent approval of variations to scientific medicinal product information relating to identified novel or increased risk (Urgent Safety Restrictions);

- Detailed assessment and investigation into locally reported incidences of severe unexpected medicinal product toxicity or any anomalous lack of efficacy following medicinal product administration (Local Product Safety Issues);

Chapter 1

Overview

- Review of newly emergent data concerning safety evidence of a medicinal product, substance or class upon request;

- Review of queries that may be related to a possible safety issues with a medicinal product, substance or class;

- Issue of Safety Circulars and Media Statements addressed to healthcare professionals and the general public respectively. These documents normally give recommendations on medicinal product use and applicable cautionary and precautionary measures. This year the Medicines Authority has introduced an SMS notification service whereby subscribed medical and healthcare professionals can receive alerts and links to the safety circulars as soon as they are published on the website.

Figure 1 below gives the distribution of reviews, communications and approvals which the Medicines Authority post-licensing directorate handled over 2011.

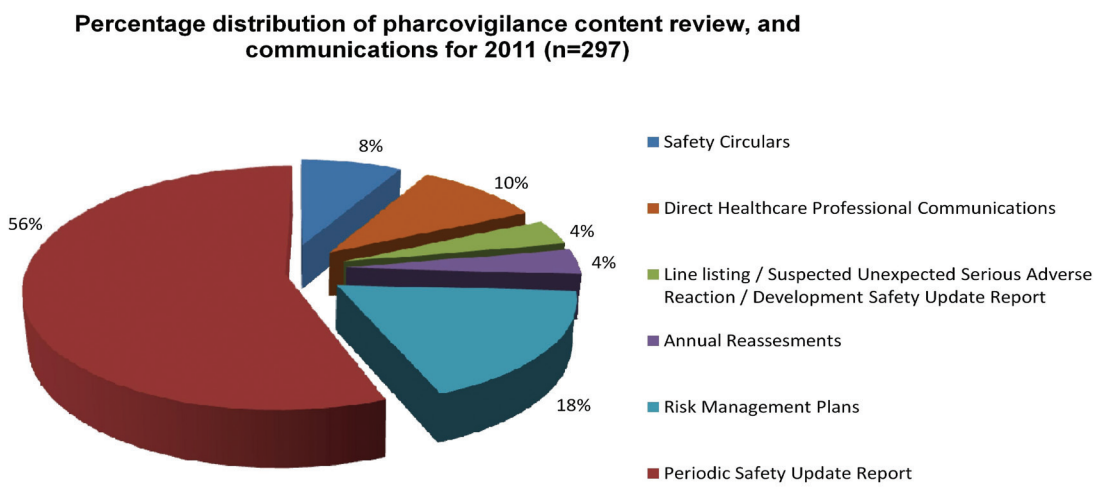


Figure 1: Distribution of Pharmacovigilance & safety issue reviews & communications

Coupled with this, the Medicines Authority's post-licensing department attends to any queries related to pharmacovigilance activities. In 2011, the main area of queries were those relating to the collection, assessment and reporting of local adverse drug reactions by healthcare professionals and Marketing Authorisation Holder representatives (Figure 2).

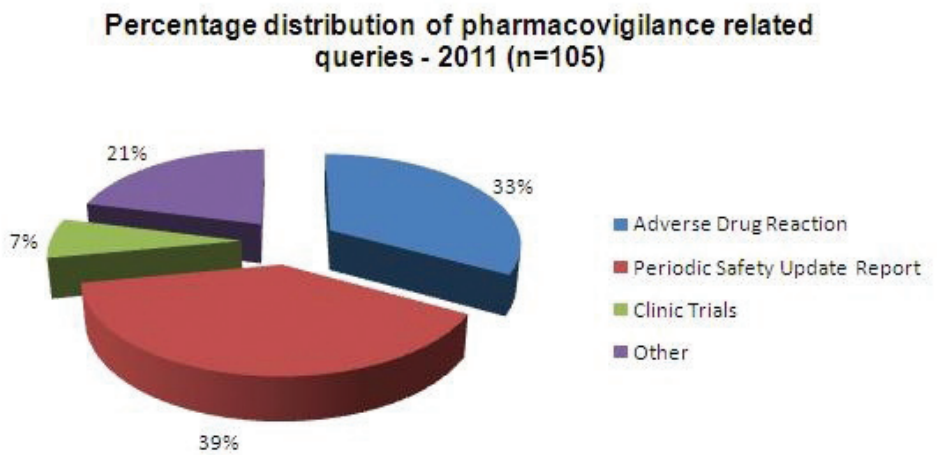


Figure 2: Percentage quantity of Pharmacovigilance related queries in 2011

The Medicines Authority also has the responsibility of inspecting and authorising pharmacies. The Authority took over this responsibility from the Department of Public Health in August 2005. Pharmacies inspections are made every two years. During 2011, the Inspectorate and Enforcement Directorate carried out the remaining pharmacy inspections of the 2010-2011 cycle, totalling to 149 retail pharmacy inspections. Therefore between 2010 and 2011 all the community retail pharmacies were inspected for the second time on a two year cycle started off in 2008. In 2012, the two-year cycle of inspections for pharmacies will start again, resuming those pharmacies which were inspected in 2010.

Another eight inspections were carried out in relation to new licences. Four new community retail pharmacy licences were inspected. Mater Dei Pharmacy and St. Vincent de Paul's Residence Pharmacy were also inspected. One new In-patients Pharmacy licence was issued as well for a private hospital. Six inspections following variation applications for pharmacy premises transfers or alterations were carried out whilst four administrative variations for pharmacy licences were processed.

In 2011, six new applications for a community retail pharmacy licence were submitted and three new applications for hospital pharmacies were also received.

Chapter 1

Overview

Furthermore, the Medicines Authority has a national public health remit with respect to pharmaceutical activity, information and use of medicinal products on the local market. Thus, appropriate rational use of medicines is a goal that needs to be achieved, so that medicines are prescribed, dispensed or sold appropriately, as well as taken correctly by patients, since the overuse, underuse or misuse of medicines results in wastage of scarce resources and widespread health hazards. The continuously updated Medicines Authority website is used as a source of independent information on medicines contributing to public education about medicines. The Medicines Authority also gave input into the National Guidelines for the use of medicines and other relevant guidelines being prepared by the Superintendence of Public Health.

Moreover, the Medicines Authority is actively participating in the government better regulation strategy. This strategy aims at improving the quality of legislation, by enhancing the performance, cost-effectiveness, legal quality of regulations and the administrative procedures, tariffs and fees derived there from. Staff from the Medicines Authority attended training organised by the Better Regulation Unit. An exercise was carried out to cost the simplification initiatives implemented by the Medicines Authority between 2008 and May 2011. The results showed that simplification measures adopted by the Medicines Authority resulted in a saving of approximately 200,000 Euro to the industry. The simplification initiatives included accepting information as a soft copy and reviewing the frequency of inspections.

1.2 Organisation Structure

The Medicines Authority is presently composed of the units listed below:

- **Office of the Chief Executive Officer (CEO)** - The office of the CEO vests the legal and judicial representation of the Medicines Authority. The CEO has the overall responsibility of the leadership, management and performance of the Authority including the management of the day-to-day operations of the Authority and overall achievement of planned targets.

- **Licensing Directorate** - The Licensing directorate processes all applications for product pre-authorisation and post-authorisation activities through established National and European procedures. This includes the variation, revocation or suspension for all product related licences and authorisations. The directorate also processes applications for work-sharing of European procedures.

- **Post-Licensing Directorate** - The Post-Licensing directorate is responsible for the constant monitoring of the safety of medicines after authorisation ('pharmacovigilance' and 'advertising'). The Medicines Authority receives safety reports from within the EU and outside concerning authorised medicinal products and acts upon the information relating to the safety and quality of medicinal products.

- **Inspectorate and Enforcement Directorate** - The two main activities of the Inspectorate and Enforcement Directorate are inspections of wholesalers, manufacturers/importers and pharmacies, their licence renewals and variations plus the remit to carry out enforcement activities in line with the Medicines Act 2003 and its subsidiary legislation.

- **Finance and Administration** - The Finance and Administration Unit plans, organises, directs and controls finance related matters including the issue of management accounts, budgets and liaison with external auditors. It is responsible for all procurement, travel arrangements and the drafting and maintenance of Medicines Authority contracts. It is also responsible for the recruitment process and for the overall administration of the Medicines Authority.

- **Quality Management** - The Quality Management Unit is responsible for the overall quality system of the Authority and to ensure that quality management is implemented in all areas. The Quality Manager is responsible to plan and execute the internal audit programme of the Authority and to ensure that there is a system of continual improvement through the follow up of corrective and preventive action and Management Review. The Quality Manager coordinates the Benchmarking of the European Medicines Agency (BEMA) exercise of the Authority and ensures that follow up action is done.

- **Information Systems** - The role of the Information Systems Unit is to deploy and maintain a robust and secure Information and Communication Technology (ICT) infrastructure and application functionality to support the operations of the National Competent Authority and legislation regulating the local pharmaceutical sector. Moreover, new developments within the EU Telematics Programme are monitored to ensure that Information Systems (IS) comply with EU Directives.

Chapter 1

Overview

- **Operations and Regulatory Affairs** - The Operations and Regulatory Affairs Unit is responsible for relevant corporate operations and the overall planning, monitoring and support of the operations and regulatory affairs at the Medicines Authority. The Unit is responsible for EU and local regulatory affairs, customer satisfaction, corporate communications, corporate risk management, corporate human resources management, training, development, occupational health and safety of employees at the Medicines Authority. The Unit is also responsible for certain horizontal operations, other government and Authority's specific initiatives such as Better Regulation and Green Initiatives and other tasks/projects as delegated by the CEO.

The Authority's premises are located in Gzira and consist of a number of offices spread on a whole floor of a building. The Medicines Authority has a staff compliment of 42 employees, of which 35 are full-time, one is part-time, three are working on reduced hours and three employees are on a contract for service. As shown in Table 1 below, most of the Authority's staff are technical staff such as clinical assessors and pharmacists.

	Full-time	Part-time	Reduced Hours	Contract for Service
Management	6			
Technical	19	1	3	3
Administration	10			

Table 1: Human Resources at the Medicines Authority

The organisation chart in **Appendix A** depicts how the Medicines Authority is set up.

1.3 Legislation

The Authority carries out its functions under the Medicines Act (Chapter 458).

The Authority's functions are also regulated by a number of legal notices as listed below:

General

- Legal Notice 358 of 2003: Commencement notice
- Legal Notice 359 of 2003: Commencement notice
- Legal Notice 334 of 2004: Delegation to Medicines Authority Order, 2004

Licensing

- Legal Notice 437 of 2004: Parallel Importation of Medicinal Products Regulations, 2004
- Legal Notice 490 of 2004: Clinical Trials Regulations, 2004 amended by Legal Notice 248 of 2007: Clinical Trials (Amendment) Regulations, 2007
- Legal Notice 379 of 2005: Herbal Medicinal Products Regulations, 2005
- Legal Notice 393 of 2005: Medicinal Products (Labelling and Packaging) Regulations, 2005
- Legal Notice 325 of 2006: Medicinal Products (Package Leaflets and Labelling) (Transitional Arrangements) Regulations, 2006 amended by Legal Notice 253 of 2010: Medicinal Products (Package Leaflets and Labelling) (Transitional Arrangements) (Amendment) Regulations, 2010
- Legal Notice 324 of 2007: Medicines (Marketing Authorisation) Regulations, 2007
    - Amended by Legal Notice 231 of 2008: Medicines (Marketing Authorisation) (Amendment) Regulations, 2008
    - Amended by Legal Notice 252 of 2010: Medicines (Marketing Authorisation) (Amendment) Regulations 2010
- Legal Notice 368 of 2007: List of Active Substances in a Medicinal Product (Requirement of Prescription) (Repeal) Regulations, 2007

Post-Licensing

- Legal Notice 380 of 2005: Medicinal Products (Advertising) Regulations, 2005
- Legal Notice 61 of 2006: Pharmacovigilance Regulations, 2006

Manufacturers

- Legal Notice 485 of 2004: Good Manufacturing Practice in Respect of Medicinal and Investigational Medicinal Products for Human Use Regulations, 2004
- Legal Notice 381 of 2005: Manufacture and Importation of Medicinal Products for Human Use Regulations, 2005 amended by Legal Notice 252 of 2009: Manufacture and Importation of Medicinal Products for Human Use (Amendment) Regulations, 2009
- Legal Notice 119 of 2006: Good Clinical Practice and Requirements for Manufacturing or Import Authorisation of Investigational Medicinal Products (Human Use) Regulations, 2006

Wholesale Dealers

- Legal Notice 386 of 2005: Wholesale Distribution of Medicinal Products Regulations, 2005

Chapter 1

Overview

Pharmacies / Dispensing

- Internal Control of Dangerous Drugs Rules: Legal Notice 292 of 1939 as amended Drugs (Control) Regulations: Legal Notice 22 of 1985 as amended
- Licensing Fees for Private Medical Premises Regulations: Legal Notice 143 of 1998
- Pharmacies (Opening Hours) Rules, Legal Notice 476 of 2010
- Legal Notice 365 of 2005: Methadone Rules, 2005
- Legal Notice 292 of 2006: Prescription and Dispensing Requirements Rules, 2006
- Legal Notice 67 of 2007: Prescription Forms for Free Medicinals Rules, 2007
- Legal Notice 243 of 2007: Authorisation of Dispensing of Medicinal Gases from Premises other than a Pharmacy Rules, 2007
- Legal Notice 279 of 2007: Pharmacy Licence Regulations, 2007
    - Amended by Legal Notice 81 of 2008: Pharmacy Licence (Amendment) Regulations, 2008
    - Amended by Legal Notice 198 of 2010: Pharmacy Licence (Amendment) Regulations, 2010
- Legal Notice 235 of 2008: Dispensing of Medicinal Products (Foundation for Social Welfare Services) Rules, 2008
- Legal Notice 188 of 2009: Rules of 2009 on the Provision of Medicinal Products through the Genito Urinary Clinic within the Government Health Services
- Pharmacies (Opening Hours) Rules. LN 476 of 2010

Fees

- Legal Notice 260 of 2004: Qualified Person (Fees for Application) Regulations, 2004
- Legal Notice 315 of 2006: Medicines Authority (Fees) Regulations, 2006
- Legal Notice 427 of 2007 [under the EURO ADOPTION ACT, 2006 (ACT X of 2006)]: Adaptation of Laws (Chapters 451-492) Order, 2007
- Legal Notice 236 of 2008: Pharmacy Licences (Fees) Regulations, 2008
- Legal Notice 29 of 2009: Health Ethics Committee (Fees) Regulations, 2009

Other

- Legal Notice 474 of 2004: Colouring Matters in Medicinal Products for Human Use Regulations, 2004
- Legal Notice 80 of 2006: Government Health Services (List of Medicinal Products) (Repeal) Regulations, 2006
- Legal Notice 264 of 2006: Special Procedure (Penalties in respect of the Medicines Act) Regulations, 2006
- Legal Notice 60 of 2008: Medicines Products (Injunction to Advertising) Regulations, 2008
- Legal Notice 58 of 2009: Availability of Medicinal Products within the Government Health Services Regulations, 2009

1.4 ICT at the Medicines Authority

Considering the extensive amount of data managed by the Authority, information is undoubtedly one of the most important assets at the Medicines Authority.

The IT Systems used at the Medicines Authority are:

- **Malta Drug Information System (MDIS)** - MDIS is the core information system used by the Medicines Authority. It is a repository of all medicinal products licensed by the Authority.

- **Sage Line 50** - The main accounting package used by the Authority to keep track of supplier invoices and all financial transactions.

- **Dakar Payroll** – The Payroll system provides a complete payroll processing of both full-time and part-time Authority employees. This includes the maintenance of the Authority's employee details through the management of leave, actual payroll calculation, printing of payroll reports and payslips, processing of direct credit payment and submission of periodical Final Settlement System returns as required by the current legislation.

- **Dakar Time & Attendance System (hardware and software)** - Time and attendance system used to record employee attendances. This system automates the capture and allocation of employee time and attendance information into the Payroll System.

- **European Union Telematics Systems** - The Medicines Authority utilises a number of European Information Technology application systems. These are web-based systems hosted at the European Medicines Agency (EMA) in London. The Authority has a secure Virtual Private Network (VPN) connection to London to access these systems. The Medicines Authority collects safety information from local healthcare professionals including occurrence of adverse drug reactions to medicinal products available on the market or at hospital. Such data is inputted in these European IT applications such as EudraVigiliance (EV) and EV Data Analysis System (EVDAS). The Medicines Authority also implemented the European Pharmacovigilance Issues Tracking Tool which is an online system that allows specialists within the EU to track product-related pharmacovigilance safety issues.

Chapter 1

Overview

- **Intranet** - The Authority operates an Intranet referred as the LinkLibrary, which hosts a large number of internal documents, standards, circulars etc. and acts as a repository of information for the Authority's employees.

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

- Malta Drug Information System;
- EU Telematics Systems; and
- Intranet.

The ICT Infrastructure at the Medicines Authority consists of:

- **Servers and Storage Hardware** - The Authority uses servers/virtual machines provided by the Malta Information Technology Agency (MITA). Office Automation storage is also provided by this same third party supplier.
- **Personal Computers (PC)** - The PCs were acquired through the government leasing agreement through the Ministry's Information Management Unit. All workstations at the Medicines Authority include an energy-efficient computer and a 19" TFT monitor. As part of a wider strategy to reduce the use of paper, quality assessors were provided with a second TFT screen. (This initiative proved to be very successful as the Authority reduced the overall use of paper by 26%).
- **Network** – The Local Area Network (LAN) switches were provided and are being supported by MITA. A fibre optic link connects the Authority to Malta Government Network (MAGNET).
- **Electronic mail (E-mail) System** - The Authority uses MITA's e-mail system.
- **Office Automation Software** - Microsoft software licenses are acquired through MITA.
- **Telephone System** – A Private Automatic Branch eXchange (PABX) is in place.

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

1.5 Audit Scope and Objectives

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

The IT Audit carried out consisted of three different stages:

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

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

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

Therefore, the objectives of this report were to:

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

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

- Determine whether the Medicines Authority's IT systems operate effectively, efficiently and economically;

- Record the findings and identified related risks; and

- List the recommendations.

Chapter 1

Overview

1.6 Audit Methodology

In order to attain the above objectives a number of interviews were held with the IS Manager and other officials at the Medicines Authority.

Reference was also made to the Control Objectives for Information and related Technology (CoBit) set of best practices. CoBit is a comprehensive set of resources that contains all the information organisations need, so as to adopt an IT governance and control framework. CoBit provides good practices across a domain and process framework in a manageable and logical structure to help optimise IT-enabled investments and ensure that IT is successful in delivering against business requirements. The CoBit framework consists of four IT domains and 34 IT processes. The controls that were considered during this audit are listed in **Appendix B**.

1.7 Structure of the Report

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

- Chapter 2 deals with the IT management perspective;
- Chapter 3 reviews the Medicines Authority's suite of software application in greater detail;
- Chapter 4 evaluates the Protection of Information Assets;
- Chapter 5 assesses the risk management, business continuity and disaster recovery procedures; and
- Chapter 6 lists the management comments.

1.8 Acknowledgements

NAO would like to express its appreciation to all the staff within the Medicines Authority, who were involved in this audit, particularly the CEO and the IS Manager for their time and assistance.

Chapter 2

IT Management

2.1 Information Technology Unit

The Medicines Authority has an Information Systems Manager who was appointed in 2004 to manage the IT Unit, co-ordinate projects and provide technical support tasks. Between 2004 and February 2006 this unit had an IT officer who left but was not replaced.

The Information Systems unit operates and maintains the existing in-house and European Information Systems and the ICT infrastructure. In 2011, two Requests for Information (RFI) were issued to obtain information on an Integrated Licensing Management System and on Digitalisation of Scientific Dossiers. Furthermore, the network switches and the router to connect to the Malta Government Network were upgraded.

The Medicines Authority is currently working on a tender for a Licensing System and the process to develop the tender document started with the support of the MITA.

The Medicines Authority has also issued and adjudicated a tender for the development of a new corporate website which will include enhanced functionalities for the Malta Medicines List. The NAO is informed that this website is expected to be implemented in the third quarter of 2012.

The Authority's IT requirements are discussed in various management meetings, Information Systems meetings, corporate staff meetings and in the communications and public relations working group. Furthermore, every quarter a management meeting is held where IT related items are sometimes discussed. Moreover, IT meetings are held separately when required. The NAO noted that, during 2011, two IT meetings were held.

A Management Review is also held once mid-yearly during which IT is one of the aspects reviewed.

Although the Authority is a small entity and almost all IT needs are supported by MITA, NAO believes that the functions of the IT unit should not be dependent on one member of staff. Another member of staff should be trained so as to step in if required.

2.2 IT Strategy

As the Medicines Authority does not have a formally documented IT strategy, the Authority adopted the Operational Plan template used within the public sector which includes a list of the objectives together with the planned Information Technology and Information Systems projects. This operational plan also includes the details of the person accountable for each deliverable within this plan.

The planned objectives for 2011 were:

- Finalisation of the RFI for the Scanning of Dossiers and issue of tender in line with management decision;

- Licensing System:
  - Working group for Licensing system to update management with progress on a quarterly basis;
  - RFI and recommendation on way forward;
  - Decision to be finalised by Quarter three;
  - Implementation to start in Quarter four (e.g. tender/ negotiated procedure). If not achieved to procure only review tool (e.g. EiY/ Docubridge) by Quarter three.

- Procure Adobe Pro for users as indicated by line managers;

- Ongoing support to desktop users;

- To come up with integrated IT solutions which are doable within available resources and set time frames;

- Responsibility for digitalisation project (started). If server space is not available, project to continue considering alternatives;

- Follow up issues at Telematics Committee/Working Groups;

- Ensure availability of server space as needed;

Chapter 2

IT Management

- Responsibility for Website Project (started):
  - Finalisation of Website Framework by Quarter three;
  - Malta Medicines List to be transferred to new website;
  - Electronic submission and payment by end of year;
  - All content to be reviewed and uploaded by end of year.

- Launch of the new website;

- Structure and reorganisation of website, intranet and server through an effective document management system.

The above objectives were all achieved apart from the responsibility for the digitalisation project and the scanning of the dossiers which were shelved due to cost.

Apart from the operational plan mentioned above, the authority lists the IT targets as part of its Business Plan.

The NAO suggests that the Medicines Authority has a formally documented IT strategy that:

- Makes reference to the Information Technology and Information Systems projects and improvements listed in the operational plan and explains how these projects are linked to the Medicines Authority's Business Strategy, and how these projects are going to be implemented;

- Covers the developments being planned in the next three to five years; and

- Refers to the Logical and Physical architecture of the Medicines Authority's IT systems.

2.3 IT Budget

The Medicines Authority's IT budget is allocated as per Table 2 below:

	2010 (actual)	2011 (actual)	2012 (planned)
New IT Investment	€242	€47,460	€1,270,000
IT Support	€11,780	€13,794	€13,114

Table 2: IT Budget

During the course of this audit and as documented in Section 2.5 below, the IT services provided by MITA are covered by a Ministry contract and not a contract specific to the Medicines Authority. Thus, the Actual Budgets for 2010 and 2011 do not include the cost of the PC leasing agreement, and the cost of IT support paid to MITA.

The NAO also observed the difference in the actual expenditure for new IT investment in 2010 and 2011. Reviewing the line items making up these figures NAO noted that in 2010 the Authority's only IT investment was a Visio software application licence. However, in 2011 the Authority procured Adobe and Windows Server licences, signed a contract for a new website, procured an IT System and paid for consultancy work in connection with issuing a tender for a new IT System.

The NAO also observed the high budget for the new IT investment planned in 2012 and thus reviewed its makeup. NAO noted that the bulk of this budget is made up of the procurement of a new licensing system.

The NAO recommends that as a best practice, the Medicines Authority carry out an exercise to analyse the cost/benefit of its Information Technology and Information Systems operational costs. This analysis would be one of the important factors in the decision process for the future planned Information Technology and Information Systems procurement.

Chapter 2

IT Management

2.4 Project Life Cycle

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

2.4.1 Hardware project life cycle

As detailed in 2.6 below, the Medicines Authority procures most of its IT equipment through the PC leasing scheme. Other IT equipment, which may be needed, but is not covered under such agreement, is procured by the IT Unit. The procurement process is kicked off with a requisition order which is sent to the IT Unit. The IT unit then reviews together with the CEO the business case for the procurement requested. Once accepted, the IT Unit gathers quotations for the items required and the successful supplier is selected. The necessary approvals are then obtained in order to procure the items in question.

Since the Authority opted for the procurement of PC's through the PC leasing scheme, the Authority's old PC's were disposed of as per the leasing agreement.

Other IT Assets that are to be disposed of are first certified by a technician as beyond economic repair and then a Board of Survey is set up and the disposal of asset is documented.

The NAO recommends that the Authority adopts the Desktop Services Procedure (GMICT R 0084:2009)[1] in terms of PC Disposal and Data Wiping, so as to ensure that deleted data may not be retrieved by any third party.

2.4.2 Software project life cycle

The NAO observed that the software used by the Medicines Authority up to now, is either off-the-shelf software or legacy systems upon which no enhancements were made. The Authority therefore does not have a formally documented software project life cycle which it follows.

The NAO thus recommends that the Authority follows a software project life cycle whereby it has a structured way of building / procuring new IS and documenting the steps to be followed when enhancements to these systems are made.

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

The Software project life cycle should include the:

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

The NAO observed that the Medicines Authority still went through all the above mentioned phases whilst procuring and implementing their new website.

2.5 Third Party Suppliers

The Medicines Authority has entrusted MITA, being the ICT Agency for the Government of Malta, with the provision of all core services in line with the Office of the Prime Minister (OPM) Circular No. 29/2005.

MITA provides the Medicines Authority with a fibre optic connection to the MAGNET and provides 24/7 monitoring of this connection. Furthermore, MITA is providing the Medicines Authority with the below listed services:

- E-mail;
- Internet browsing and filtering;
- Standard desktop security configuration services, such as anti-virus 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; and

- First line support for the resolution of incidents reported to MITA's Service Call Centre regarding the above mentioned services.

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

The Medicines Authority however has contracts and service-level agreements with other suppliers. The NAO reviewed all these contracts and agreements and recommends that the Medicines Authority ensures that all contracts and agreements:

- Call for the Medicines Authority and not the Medicines Regulatory Unit or Medicine Authority or any other name variant;
- List the correct address;
- Are still valid and in the case of long term contracts which are renewed automatically, the Authority should ensure that these contain a clause stating that these are automatically renewed from year to year;
- Contain suitable Data Protection Clauses. The sample clauses issued by OPM so as to guide government departments/entities in this regard can be used;
- Rates are still valid. The Authority should ask suppliers to send a notification of rate changes in writing, so that rates paid are in agreement with those specified in contract;
- Are in Euro and if stating a VAT Rate this is up-to-date with the current legislation. i.e. A contractor stating that the invoice should be paid in Lm or that payments are subject to 15% VAT, should be revised; and
- List the completion dates of projects.

The Medicines Authority should also ensure that contracts are kept up to date and if need be a covering letter documenting changes and signed by both parties should be done. Furthermore, the Medicines Authority should ensure that all third party suppliers abide by the terms and conditions in the contracts, especially when it comes to delivery dates and call-out rates charged.

2.6 PC Leasing Scheme

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

During March 2010, the Medicines Authority replaced all desktop computers and laptops through the PC leasing Scheme. Requests of maintenance and repairs are now being handled by MITA through the Information Systems Manager and serviced by the third party suppliers who were awarded the tender.

Although this scheme has brought a number of benefits to the Authority, both the NAO and the Authority itself, acknowledge that this scheme has also created a number of risks and limitations.

Primarily, since computers are now being serviced and repaired by third party suppliers, computers may need to be taken out of the Authority's premises to the third party's workshop. Due to the fact that all hardware is relatively new, the need to have hardware serviced outside the Authority's premises has never occurred as yet. Yet this still presents a risk to the Authority, since the hard disks of the Authority's computers may contain confidential data.

Secondly, the computers are now assigned to employees and therefore when an employee is transferred to another government entity, he/she is expected to transfer his/her computer. NAO recommends that the Medicines Authority implements procedures to identify and erase any sensitive information and software stored inside its computers, disks and other equipment, before being transferred to another Government entity. This would mitigate the risk of unauthorised access to sensitive data which may reside in the above mentioned equipment.

Chapter 2

IT Management

2.7 Network Infrastructure

The Authority is connected to the Government Network generally referred to as MAGNET, via a 10 Megabits per second (Mbps) fibre optic link to MITA-01 Data Centre in St. Venera. Network connectivity is monitored and maintained by MITA on a 24/7 basis. MITA also maintains all network hardware, including the Authority's router, and provides the necessary support accordingly.

Internally, the Medicines Authority operates a LAN based on two switches and Unshielded Twisted Pair cabling. The Authority's LAN is also monitored and supported by MITA.

As part of this audit, NAO requested a Network Diagram and reviewed the network setup. NAO observed that all networking equipment is connected to a Uninterrupted Power Supply (UPS) which is regularly tested by the Information Systems Manager.

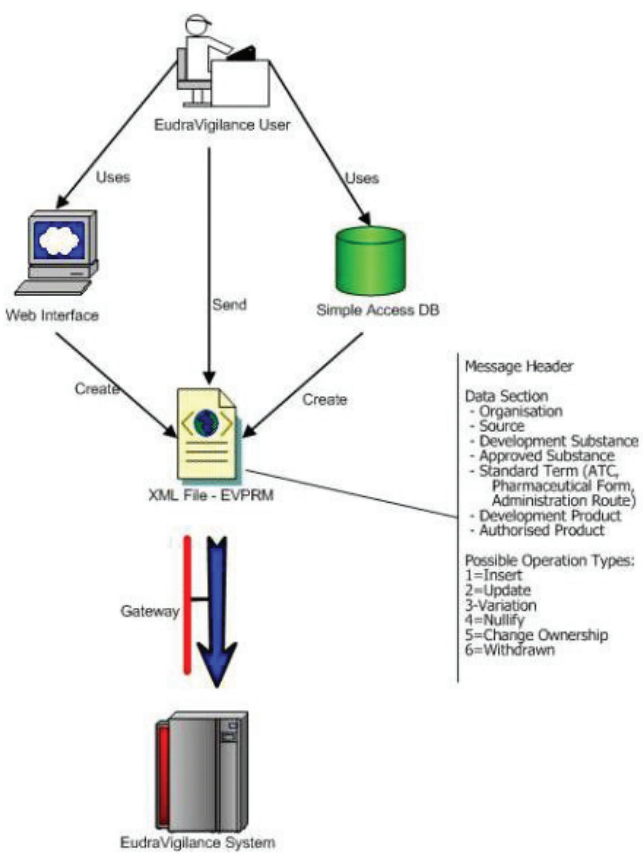


Figure 3: EudraVigilance Data Collection Process[2]

[2] http://eudravigilance.ema.europa.eu/human/evMpd03.asp

Furthermore, the Medicines Authority has a VPN connection (known as EudraNet) to the London office of the EMA, to access the EU Telematics systems. EudraNet is a European human and veterinary pharmaceuticals communications network offering ICT services that provides scientific experts and those working on pharmaceutical business processes and policy makers, with a secure and well-structured electronic environment to exchange information.

EudraNet provides appropriate secure services for inter-agency data interchange and for exchanges between Agencies and industry. Its main objectives are:

- One of EudraNet's main objectives is to enable the electronic exchange of information between the European Commission, EMA and the national regulatory authorities responsible for pharmaceuticals across the EU Member States.

- A second key objective is to provide a service for secure and managed communication over the Internet between European Agencies and pharmaceutical companies. This has been achieved through the implementation of EudraLink, a software tool designed to facilitate the secure transmission of information or documents between the EU Member States, the European Commission and the pharmaceutical industry. Thanks to EudraLink, elements of the marketing authorisation procedures can now be carried out over the Internet. EudraLink seeks to ensure the confidential and rapid granting of these authorisations.

- Thirdly, EudraNet exists to host and provide access to Community databases in pharmaceuticals. This includes the European Experts Database and Pharmacovigilance database (EudraVigilance) Figure 3 above.

- Finally, and most importantly, EudraNet aims to provide a collaborative work environment and business cooperation tools such as virtual meetings.

The router supporting this VPN connection is maintained conjointly by the Information Systems Manager and the EMA who log into it using the pubic Internet Protocol (IP) address and make any necessary maintenance.

NAO also held a site inspection in the Authority’s computer room and observed that at the time of the inspection:

- The door was unlocked;

- The air conditioning unit was switched off;

Chapter 2

IT Management

- The network cabinet was overcrowded with equipment and needed reorganisation of the cabling within the cabinet.

NAO was informed that the computer room is usually locked and that the air conditioning unit in the room was switched off during the winter months.

NAO thus recommends that:

- A larger network cabinet is procured so as to reorganise all the network and telephone cabling in an orderly fashion making them manageable;
- Any unnecessary or redundant equipment, such as the old server rack which is now unutilised, is removed from the computer room;
- The air conditioning is kept on throughout the year;
- A temperature and humidity monitor is installed so as to ensure that there are no temperature variances;
- The room is kept locked at all times;
- A log book is kept recording who accessed the room and the date and time; and
- An adequate fire extinguisher is placed in the room.

2.8 IT Inventories

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

The Medicines Authority has an inventory of all PCs and a Fixed Asset Register documenting all assets room by room. The NAO has reviewed both registers and suggests that the:

- Fixed Asset Register is updated i.e. The Register of the computer room still contains the servers and does not contain the network cabinet;

- PC Register includes all the devices that the Medicines Authority may have such as scanners, UPS's, external hard drives, external Digital Versatile Discs (DVD) writers, projectors and all monitors; and

- PC Register is updated in terms of ownership. i.e. NAO noticed that there are 2 particular PC's that are still registered on employees who no longer work with the Authority.

The Medicines Authority also has an inventory of software licences. The NAO has reviewed this inventory and noticed that it does not include the Microsoft Office licences, the Microsoft Windows licences, the Microsoft Windows Server licences and the Standardised Query Language (SQL) server licences. NAO thus suggests that this register is updated accordingly so as to be able to account for all software licenses being paid, as well as to make sure that all licenses are being made use of.

Chapter 3

IT Applications

Europe is the world's largest pharmaceutical producer and thus the pharmaceutical sector in Europe is extensively regulated with the dual objective of protecting public health and meeting the demands of the Internal Market.

Information Technology and Information Systems help the local Medicines Authority and the European Pharmaceutical Authorities in all stages of their business processes. Through the use of IT and IT Applications these authorities have a secure and well structured environment to "meet", exchange information and work together on a pan-European Scale.

This chapter delves into the IT Applications being used by the Medicines Authority. It includes both the IT software owned by the Medicines Authority and other software, which although owned by the EMA and not owned by the Medicines Authority, the Authority is using in collaboration with other European Pharmaceutical Authorities so as to be able to work together and reach their common objectives.

3.1 Software Applications

3.1.1 Maltese Drug Information System

The Maltese Drug Information System (MDIS) was acquired by the Medicines Authority from the Irish Medicines Board in 2003 and is managed by the Information Systems Manager who acts as an Administrator. The Information Systems Manager adds new users, assigns the necessary user rights, terminates access and does all administrative tasks concerning this application. The NAO recommends that should more staff be allocated to the IT Unit, these functions are distributed amongst different members of staff so as to avoid any conflict of interest.

The MDIS is a database of all medicinal products licensed by the Authority. The back-end is an SQL database, which is being hosted at MITA, while the front-end is written in Visual Basic and installed on every PC. Although the Medicines Authority has the source code of this system, this database was always used as procured and no enhancements or upgrades were implemented. Moreover, since this application is meant to be replaced, the Authority does not intend to upgrade or enhance this system.

The NAO noted that system documentation manuals are available. Such documents include step-by-step guidelines as to how the MDIS Client is installed and how the administrator carries out user administration, group administration and application administration tasks

documenting both the client installation and the administrator processes of this system. These guidelines also include print screens illustrating these steps.

Furthermore, NAO noted that the Medicines Authority also has the database schema of the application.

Although a user manual is not available, the Medicines Authority has compiled a set of Standard Operating Procedures (SOP's) that define the procedures for Case Managers, Quality Assessors and Medical Assessors for the input and updating of data into the MDIS. By using this SOP, the Medicines Authority aims to achieve uniformity in the data inputted in MDIS and enhance standardisation; so that the information retrieved from the system is accurate and can be used to trace the progress of applications and to report effectively to both administration and management. Furthermore, new employees are trained on the job by their experienced colleagues, who would go through the application and demonstrate how it is used.

During the course of this audit, NAO enquired about the manner in which data is received from third parties and was informed that whilst in the past almost all the data was received in large volumes of hard copy paper files, nowadays the bulk of this data is received on Compact Discs (CD's) or DVD's. Hard copies and soft copies are currently being stored in three separate rooms dedicated for this purpose. The NAO recommends that the Medicines Authority looks into the feasibility of having a web portal service through which this data can be inputted directly into the system by the provider. This facility would:

- Reduce the time taken by the Medicines Authority staff to upload the data;
- Digitalise all information avoiding problems of storage;
- Make data retention easier to control;
- Allow backups of this data to be taken; and
- Allow the provider to amend/update the data when and as required.

The NAO observed that although access to the MDIS system and its modules is controlled by a username and a password, this system has no audit trails and does not keep track of user actions. Furthermore, NAO observed that:

- There are no password rules or password complexity measures implemented;

Chapter 3

IT Applications

- Passwords do not expire;
- Old passwords can be reused;
- The system does not block access after a particular amount of unsuccessful tries;
- There is no account lockout policy in place for unsuccessful number of logon attempts;
- The users do not have a facility to reset their password; and
- Access is not terminated or disabled when an employee resigns or is away on prolonged leave.

The NAO recommends that the Medicines Authority ensures that if this system is replaced with a new system, the new system would:

- Have audit trails that record all user actions including the username, date and time when each action was performed; and
- Follow Government's password standard and password policy[3].

The Information Systems Manager explained that when an employee resigns, his/her access is not terminated because this may compromise the robustness of the system. NAO recommends that as an immediate measure, the Information Systems Manager limits the access such profiles have in such a way that although access is not terminated, logging in with such user account/password would still not give the user any access to the application's modules. This can easily be done by not linking any modules to an account which is no longer in use.

During the course of this audit NAO observed that this system has very limited functionality and is not in line with the Authority's business processes. Furthermore, NAO observed that users are creating/maintaining a number of spreadsheets so as to counter for the lack of functionality in this system. This is resulting in duplication of work and resources. NAO observed that this system has no functionality in terms of creating or maintaining a workflow, has no process alerts, does not have a report generator, does not report variations of applications, has no functionality through which one can issue a list of all

[3] Password Policy document - https://www.mita.gov.mt/MediaCenter/PDFs/1_CIMU_P_0015_Password.pdf

authorised products and is not integrated with the Medicines Authority's website. In this regard, the information that needs to be uploaded on the Authority's website may not be current. Furthermore, users using this application need to access each and every report to check the status of an application with the end result that the managers cannot monitor the number of files assigned to a particular employee. Users have also explained that due to the limited functionality, statistical information cannot be elicited from the system and thus has to be done manually.

Since the Medicines Authority is now also doing assessments on behalf of other member states, NAO suggests that the Medicines Authority carries a business process re-engineering exercise whereby all the Authority's processes are clearly identified from which a list of the functionality required from a new IT system can be elicited. Such exercise would ensure that the new system being procured would address all the business requirements of the Authority.

The MDIS is hosted on servers residing at MITA whose staff is also responsible for regular system maintenance and for ensuring that daily, weekly and monthly backups are taken. Such backup tapes are also stored in safe repositories at an offsite location. The NAO was also informed that these backups are periodically tested on a virtual environment and the last restore was successfully made on the 4th February 2012, loading the data of a few days before.

3.1.2 EU Telematics Systems[4]

The EU Telematics Systems comprise of a number of applications based on a legal requirement or have evolved from a defined need or requirement within the regulatory network.

These Systems are hosted and operated by the EMA which comes under the overall responsibility of the European Commission's Directorate-General for Health and Consumers. These applications are provided in collaboration with the EMA and the national authorities responsible for pharmaceuticals, which make 28 organisations in total including Malta. Such applications include the:

- EudraNet Services supporting the cooperation for the entire EU market and post marketing surveillance; and the

[4] Source: European Medicines Agency: Introduction to the EU telematics programme

Chapter 3

IT Applications

- Communications and Tracking System (CTS) supporting the marketing authorisation process of medicinal products through the mutual recognition procedure enforced by the European Economic Community Council Regulation (EEC No. 2309/93) and by Directive 2001/82/EC and Directive 2001/83/EC.

Both EudraNet Services and the CTS have been operational since 2004. During 2002 however, the Support to Pharmaceutical Research Unit within the Institute for Health and Consumer Protection, successfully finalised the transfer of the EudraNet Services to the EMA and the services of the EudraTrack System to the BfArM (Bundesinstitut für Arzneimittel und Medizinprodukte) regulatory Authority.

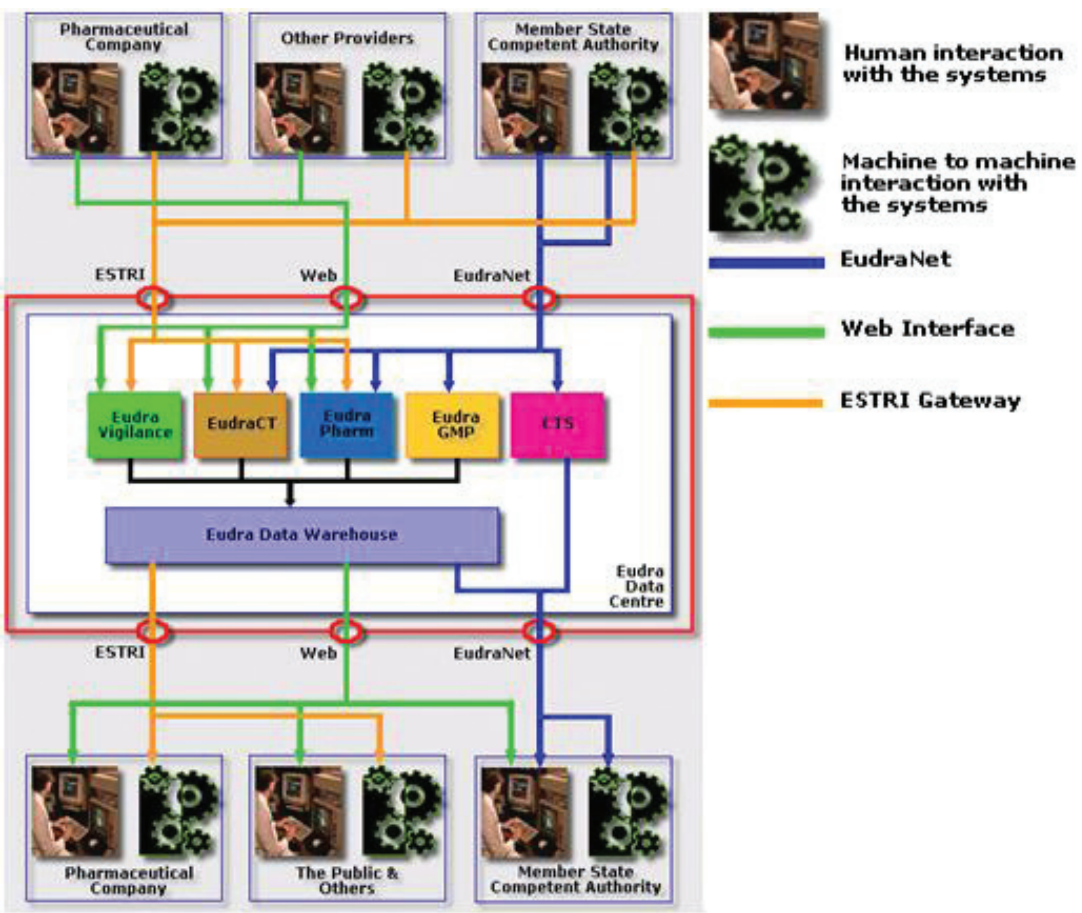


Figure 4: EU Telematics Systems[5]

[5] Source: European Medicines Agency, London, UK

The EMA has been assigned the responsibility for developing and operating European computer Information Systems as set out in the EU's strategy and implementation plan for telematics in the pharmaceutical sector. This strategy is agreed between Member States, the EMA and the Commission. It is to be considered as a Community strategy. The Telematics Steering Committee is in charge of the monitoring and development of this strategy.

3.1.2.1 EudraNet Services

EudraNet is a secure network and the backbone of the European Medicines Regulatory System. EudraNet facilitates secure communication, and also enables secure access to applications hosted at the EMA, for example, Eudra good manufacturing practice (EudraGMP). All Member State competent authorities, the European Commission and the EMA have access to this system and the system has been in full operation since 1995. Industry or non-regulatory organisations do not have access to EudraNet. There is a Technical Implementation Group in place to reflect user requirements and provide feedback on performance together with ongoing issues.

The four objectives of the EudraNet services are:

- Enabling electronic communication and sharing of information between the European Commission, the EMA, and the national competent authorities in pharmaceuticals;
- Providing a gateway for the secure and managed communication over the Internet between European administrations and pharmaceutical companies;
- Hosting and providing access to Community databases in pharmaceuticals; and
- Providing a collaborative group working environment.

More specifically, EudraNet provides network services, application services (common databases) and support services.

Chapter 3
IT Applications

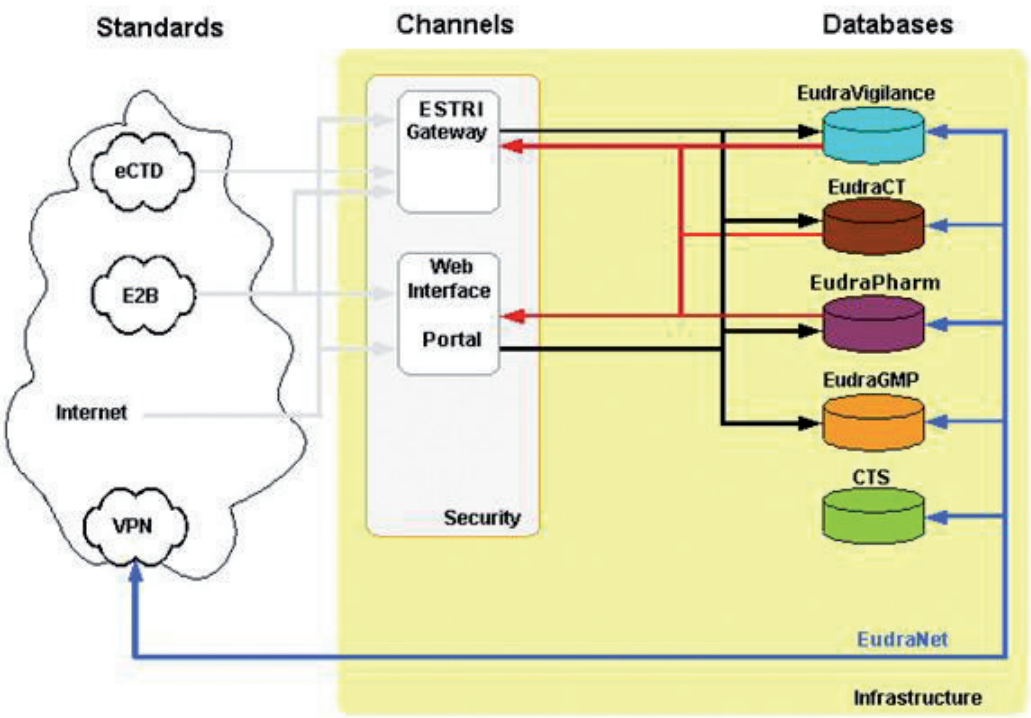


Figure 5: EudraNet Infrastructure[6]

As depicted in Figure 5 above, the network infrastructure consists of a backbone network that interconnects dedicated lines of 32 organisations: the Commission, the EMA and the national competent authorities responsible for human and veterinary medicinal products in the EU, Norway and Iceland.

In 2002, in view of the transfer to the EMA of all EudraNet activities, including both the EU Telematics systems and the Eudra network, the Support to Pharmaceutical Research undertook a major reengineering and restructuring process to streamline and consolidate all activities and systems necessary to run EudraNet.

In line with the Commission framework contract, the network consolidation process involved a major upgrade of all systems and the EudraMail relay services and also included the migration to a new Internet Service Provider. The overall security of the EU Telematics systems was also reviewed and new monitoring services were added to implement an Intrusion Detection System.

[6] Source: European Medicines Agency, London, UK

As part of the transfer activity, the EudraNet team in London prepared a series of training sessions to facilitate the learning process for the new team in charge of the EudraNet services at the EMA. In addition, the EudraNet team also provided a detailed and thorough documentation on the systems.

The training sessions, which included also introductory and tutoring components, were followed by hands-on sessions where the systems were illustrated to the EMA team.

The EMA and the Joint Research Centre signed the final EudraNet Services Transfer Agreement on 30th December 2002, with which the EudraNet equipment, the hardware on which the EudraNet runs and the commercial software used to implement Eudra services were officially transferred to EMA.

The Medicines Authority has a support and maintenance agreement with the EMA.

3.1.2.2 EudraPharm

Legal basis: Articles 57 (1) and 57 (2) of Regulation (EC) 726/2004

EudraPharm is a database designed to hold information on each medicinal product (Human and Veterinary use) authorised in the EU, and the European Economic Area. The system is required to hold the information contained in the Summary of Product Characteristics (SPC), the Package Leaflet and the labelling. Its purpose is to provide authoritative information to all stakeholders and the general public.

3.1.2.3 EudraVigilance

Legal basis: Article 6 of Directive 2001/83/EC as amended by Directive 2004/27/EC, Directive 2001/82/EC as amended by Directive 2004/24/EC, and Regulation (EC) No. 726/2004).

EudraVigilance (EV) is the EU database on adverse drug reactions that receives, processes and stores individual case safety reports for all medicines authorised in the EU, wherever in the world the adverse reaction reported occurred. The EudraVigilance Data Analysis System (EVDAS) provides the capability to analyse the data for signals. The system also receives, processes, and makes available for analysis, reported suspected and unexpected serious adverse reactions that occur during clinical trials.

Chapter 3
IT Applications

3.1.2.4 Eudra Clinical Trials

Legal basis: Article 11 of Directive 2001/21/EC and articles 41 and 53 of Regulation (EC) No. 1901/2006

Eudra Clinical Trials (EudraCT) is the EU system for the registration of clinical trials. The current project extends the functionality in line with the requirements of the Paediatric Regulation and enhancement requests from the Heads of Medicines Agencies' Clinical Trials Facilitation Group (CTFG). Key amongst the changes is the publication of results and the identification and publication of certain items relating to paediatric indications within the database. Some data on the results of clinical trials will be made available to the general public. The system is used by National Competent Authorities to monitor aspects of clinical trials being undertaken in Europe.

System development started in May 2004. The current version is version 7, which was released in 2009. Data warehouse and reporting functionality is in pilot production, linked with the Eudra Data Warehouse projects. The system is expected to be upgraded to Version 8, which includes a substantial rewrite of existing functionality, to eliminate performance and architectural weaknesses introduced through 'bolted-on' additions over the year. Furthermore, the system upgrade substantially addresses the stated requirements of the CTFG and the requirements of the Paediatric Regulation.

3.1.2.5 Eudra Good Manufacturing Practice

Legal basis: Article 40(4) of Directive 2004/27/EC and article 44(4) of Directive 2004/28/EC

EudraGMP facilitates the exchange of information on compliance with good manufacturing practice (GMP) among the competent regulatory authorities within the European medicines network. The system allows for:

- the submission of GMP certificates, manufacturing and importation authorisations by national competent authorities on-line and via an XML-based interface using the gateway;

- enables the submission of non-compliance with GMP information that results from inspection activity;

- allows the sharing of information on planned inspection activity on manufacturing sites in third countries;

- permits the consultation of the GMP, authorisation, non-compliance and inspection coordination information that results from the above submissions; and

- supports the exchange of information constituting 'rapid alerts' arising out of faulty manufacture.

The database provides public access to information about manufacturing authorisations and GMP compliance certificates. Extension of EudraGMP to accommodate the requirements of good distribution practice as an anti-counterfeit measure is also foreseen.

The system has been in production since 2007. The next version, including the sharing of information on planned inspection activity on manufacturing sites in third countries and the exchange of information constituting 'rapid alerts' arising out of faulty manufacture, is foreseen to be started in 2012. Also foreseen for 2012 is the initiation of the Good Distribution Practice Database (EudraGDP).

3.1.2.6 eSubmissions: European Union Review System

The European Union Review System (EURS) is a system that validates, stores and presents electronically submitted marketing authorisation application dossiers for review, using the functionality of the electronic Common Technical Document (eCTD) to enable information through the lifecycle of the medicinal product to be displayed according to the requirements of the reviewer. The Medicines Authority intends to implement this system in the coming months.

The system has been in production since 2006. Improvements to the national cache manager are the only activities ongoing related to the EURS itself. Linked activities, all of which are nearing completion, include establishment of the central repository and the opening of the electronic gateway at EMA. In or after 2013, a project is foreseen to integrate Product Information Management[7] into the EURS. No decision has yet been made regarding possible changes to the technology implemented on expiry of the existing contractual arrangements.

[7] Refer to 3.1.2.10

Chapter 3
IT Applications

3.1.2.7 eSubmissions: Central Repository

The Central Repository is an electronic filing area used to hold dossiers for marketing authorisation applications submitted electronically via the centralised procedure. Dossiers are held in this single location at EMA and made available electronically for review across the European Medicines Regulatory Network. Thus, reviewers may review applications held at EMA from their own desks.

3.1.2.8 eSubmissions: Electronic Gateway

The gateway for the acceptance of electronic submission of marketing authorisation applications permits the receipt of eCTD and other submissions, which are then routed to the electronic repository following validation for further processing.

This technology has been in use since 2001, for the electronic receipt and routing of individual case safety reports for pharmacovigilance.

3.1.2.9 eSubmissions: Electronic Application Form

On completion of this project, electronic forms for the submission of data in structured form as contained in the existing application forms developed through the Notice to Applicants Group and within EMA will be published. In addition, tools to create these forms, and to receive and validate them, will be available for use by applicants and regulatory authorities.

3.1.2.10 eSubmissions: Product Information Management

Product Information Management is a term that describes a new way of handling product information (the SPC, labelling and package leaflet, for authorisation) in the European regulatory context. The project is delivering:

- An exchange standard;
- Support for an all-electronic process;
- A review system for regulators;
- A validation engine for all stakeholders; and
- A light authoring tool for SME's.

The platform will be used for the submission and exchange of comments, and finalisation of product information initially within the centralised procedure, and ultimately across all marketing authorisation application procedures. Ultimately, it will serve as the authoritative source for information that is published through EudraPharm.

The Electronic Summary of Product Characteristics Proof of Concept is designed to establish the requirements of decision support systems with regard to the information in the Summaries of Product Characteristics. The project serves as a means of gathering requirements for the product information management data exchange standard.

3.1.2.11 European Union Telematics Controlled Terms

European Union Telematics Controlled Terms (EUTCT) is a central repository and publication system for controlled term lists used in the European Medicines Regulatory Network. It is designed as a support mechanism to the other projects as it provides a framework of terms to facilitate the exchange and interrogation of data across the various systems.

It comprises:

- An agreed set of controlled term lists (including, for example, country code, route of administration, Anatomic Therapeutic Chemical (ATC) code);
- A process and an infrastructure enabling the controlled update of the controlled term lists with agreed terms in a timely manner; and
- A process to provide, wherever possible, the controlled term lists to the participating stakeholders.

The system is accessible, with differing access privileges, to National Competent Authorities and other stakeholders' systems to assure consistency of use of terms throughout the European Medicines Regulatory Network, and amongst those interacting directly with the Network, for instance through application forms.

3.1.2.12 Eudra Data Warehouse

The Eudra Data Warehouse will be a collection of information related to medicinal products regulated in the EU and the European Economic Area extracted from all the systems established through the EU Telematics programme. The warehouse will serve as a data-minable repository. It is anticipated that access will be granted, according to different permission sets to partners (National Competent Authorities), stakeholders and the public in EU telematics.

Chapter 3
IT Applications

The Eudra data warehouse is currently implemented as four separate warehouses – two in full production, and two in pilot. These are:

- In production:
  - The EVDAS (for human medicinal products, in production since mid-2007);
  - The Eudra Data Warehouse for veterinary medicinal products (in production since early 2008).

- In pilot:
  - The EudraCT Data Warehouse (in pilot since quarter 3, 2009);
  - The Project 196 Data Warehouse (for human medicinal products – in final testing). This is a proof-of-concept to speed up the 'folding-in' of the functionality for human pharmacovigilance analysis, using a different architecture than currently used for EVDAS.

The Eudra Data Warehouse project is ongoing. The Project 196 technology will replace the data warehousing technology used in EVDAS. The Eudra data Warehouse for veterinary medicinal products will also assimilate Project 196 technology, and in subsequent years, the three separate warehouses will be merged into one.

3.1.2.13 European Communication and Tracking System

Legal basis: Chapter IV, title 3 of Directive 2001/83/EC & Directive 2001/82/EC, articles 27-32.

The Communication and Tracking System (CTS) is the system used by the National Competent Authorities involved in the licensing of human and veterinary medicinal products via the mutual recognition and decentralised procedures.

CTS is a tracking system that permits the registration of procedures for marketing authorisation submitted through the mutual recognition process, to Competent Authorities in the Member States of the EU. Data items relative to mutual recognition procedures (full applications and variations), are introduced by the reference and concerned Member States in a shared database that is available under controlled access to the EudraNet users. It provides a global picture of the ongoing procedures and statistical reports of those already accomplished.

The system serves as a data provider for other applications. The system has been in operation since 1995.

3.1.2.14 EMA System: European Pharmacovigilance Issues Tracking Tool

The European Pharmacovigilance Issues Tracking Tool is an EMA system that effectively tracks and monitors all Pharmacovigilance Working Party recommendations, SPC implementations and all safety issues regardless of the authorising procedure of the product, as many safety issues involve multiple medicinal products across all authorising procedures.

3.2 Web

3.2.1 Intranet

The Medicines Authority has an Intranet which is internally referred to as a LinkLibrary. This Intranet is being used as a repository of information for the Authority's employees and so as to improve the data sharing capability and overall knowledgebase of the Authority's employees.

With the use of this Intranet, the Authority's employees can download the Employee handbook, the Authority's SOP's, the Authority's Circulars and Memos, the EU Guidelines etc.

The Information Systems manager is the person who developed and maintains this Intranet. He is also the person who uploads all the data on the Intranet although this is done in conjunction with the respective line managers who are the owners of the data uploaded in this Intranet.

The Intranet is accessed through a web browser via http and restricted by IP subnet mask for internal users only.

The Intranet is hosted on servers residing at MITA whose staff is also responsible for system monitoring, regular system maintenance and for ensuring that daily, weekly and monthly backups are taken. Such backup tapes are also stored in safe repositories at an offsite location.

The NAO considers the Intranet as a potential valuable strategic asset for any organisation, as it can deliver many benefits such as an effective communication and news distribution infrastructure, supporting tool for initial and ongoing training requirements and as a platform for online community of staff.

Chapter 3
IT Applications

NAO recommends that Intranets are:

- Accessed by all employees within the entity so as to provide an efficient communication channel and increases the knowledge flow within the entity. If need be, training in this regard should be given to employees;
- Easy to use and all information uploaded is organised in such a way that it is intuitive for somebody to find it;
- Complete and incorporate all the information that employees may need i.e. incorporate all office circulars, procedures, notices etc.;
- Kept up-to-date and all content is reviewed from time-to-time so as to access its relevance;
- Secure. If need be user levels and audit trails are to be introduced. The Intranet can also be integrated with Lightweight Directory Access Protocol (LDAP) Authentication (CORP Accounts / Active Directory); and
- Easy to maintain. i.e. If the Intranet requires frequent updates, the entity should consider systems whereby this is uploaded automatically and avoid as much as possible information from uploaded manually, thus making it less labour-intensive and easy to maintain.

3.2.2 Website

The Medicines Authority has three websites as per the Uniform Resource Locator's (URL's) listed below:

- www.medicinesauthority.gov.mt
- www.knowyourmedicines.gov.mt
- www.maltamedicineslist.com

All three websites are hosted by MITA and backed up regularly.

3.2.2.1 www.medicinesauthority.gov.mt

The Medicines Authority website (www.medicinesauthority.gov.mt) is the Authority's main website through which the Authority establishes its Internet presence and provides the necessary information to stakeholders and consumers.

During the course of this IT Audit, NAO reviewed the Malta Medicines list website. NAO recommends that the site is improved as the look and feel is dated.

NAO was informed that a tender for the procurement of a new website was issued and awarded. The main functionality of the new website was developed and is currently being tested and populated with data by the Authority.

The NAO recommends that prior to going live with this new website, the Medicines Authority should ensure that this new website is in line with the Government's Website Standards GMICT S 0051[8].

Furthermore, the NAO observed that certain information in this website is out of date. For instance, the website is still advertising two vacancies that have expired in August and October 2011. The NAO thus recommends that the Medicines Authority assigns the task of updating the website to a particular employee from each section, so as to ensure that all information within the website is current, complete and up to date.

3.2.2.2 www.knowyourmedicines.gov.mt

This URL redirects the user to the Medicines Authority's Website and is in fact a page within this website. As detailed in Section 3.2.2.1 above, this website is about to be replaced with a new website.

This page is addressed to the general public and includes:

- The Medicines Regulation;
- Information regarding the safety of medicines;
- Information regarding safety and legal perspective of herbal medicines;

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

Chapter 3
IT Applications

- Downloadable information leaflets;
- Guidelines on taking medicines; and
- Information regarding product information leaflets.

Since this URL is just a page within the Authority's main website, the same recommendations in Section 3.2.2.1 apply.

3.2.2.3 www.maltamedicineslist.com

The Malta Medicines List website (www.maltamedicineslist.com) serves as an online repository listing all the medicinal products which are licensed by the Medicines Authority to be placed on the market in Malta. Through the Malta Medicines website the user may:

- Find whether a medicine is authorised to be placed on the market in Malta or not;
- Find different products containing the same active ingredient/s;
- Find different formulations of the same product or of an active ingredient; and
- Know whether a product is classified as prescription only medicine or over the counter medicine.

This website includes products licensed nationally through all routes of authorisation: marketing authorisations, authorisations in line with regulation 4(2) of the Medicines (Marketing Authorisation) Regulations and parallel import licenses and products, which are authorised by the European Commission and can be marketed in all Member States.

All authorised medicinal products are given an authorisation number depending on the route of authorisation:

- National marketing authorisations are given an MAXXX/YYYZZ authorisation number;
- Medicinal products authorised in line with regulation 4(2) of the Medicines (Marketing Authorisation) Regulations (in accordance with article 126(a) of Directive 2001/83/EC), given an authorisation number in the format of AAXXX/YYYZZ; and
- Parallel import licences which are given an authorisation number in the format of PIXXX/YYYZZ.

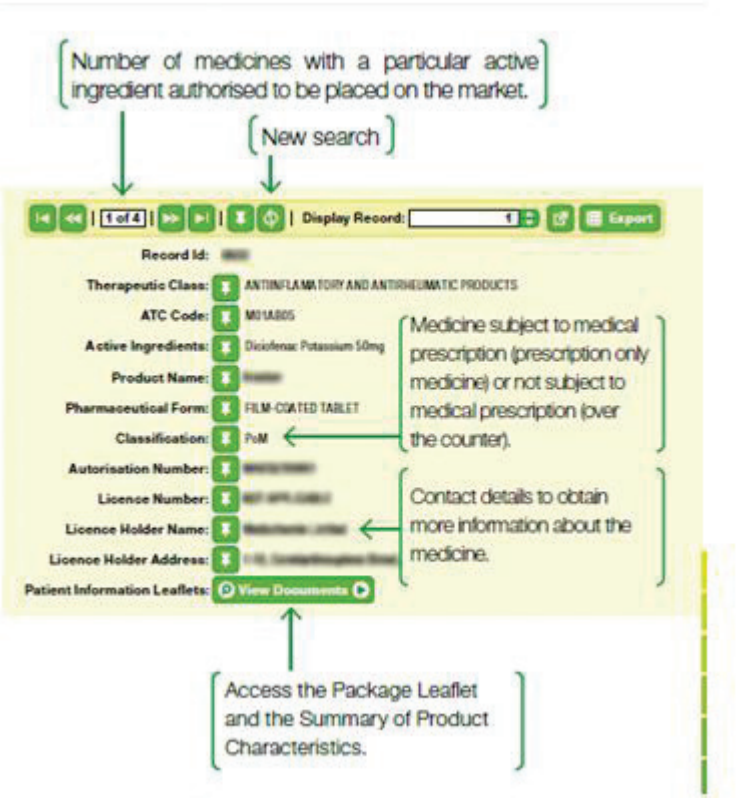


Figure 6: Malta Medicines List

During the course of this audit and whilst reviewing the Malta Medicines list website, NAO observed that upon entering this website one is greeted with a message stating “You have reached the Malta Medicines List. Please note that the page will take some time to load. Press Ok to continue” followed by another message stating “Medicines list loaded. Press Ok to continue”.

NAO also observed that whilst the website functions well, it lacks in terms of look and feel. The website is also unintuitive and an average user may not be able to grasp how it works and how to look for a product.

Furthermore, NAO observed that when the page is not maximised the fields with the page loose their position making the website unreadable and unusable if not seen in full screen.

Chapter 3
IT Applications

NAO recommends that this website is reviewed in line with modern technology and in order to improve its:

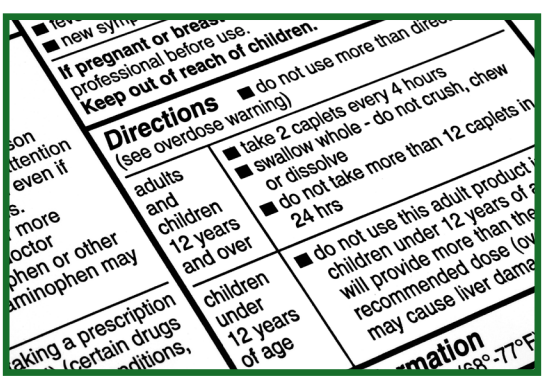
- Loading time;
- Look and feel;
- Ease of use; and
- Compatibility with different window sizing.

The Medicines Authority should also ensure that this website is compatible with all the main browsers.

Furthermore, the NAO recommends that this website is redesigned so as to comply with Government's website Standards[9] that can be downloaded from MITA's website.

[9] Government Website Standards - https://www.mita.gov.mt/page.aspx?pageid=364


M
M
T
T
F


If pregnant or breast
professional before use.
Keep out of reach of children.
Directions
(see overdose warning)
do not use more than
take 2 caplets every 4 hours
swallow whole - do not crush, chew
or dissolve
do not take more than 12 caplets in
24 hrs
adults and children 12 years and over
do not use this adult product
children under 12 years of
will provide more than the
recommended dose (ov
may cause liver dama
children under 12 years of age
aking a prescription
mation

Chapter 4

Protection of Information Assets

4.1 Anti-virus software

During the course of this audit, NAO noted that in 2010 the Medicines Authority liaised with MITA and replaced the Anti-virus Software installed on all workstations including the spare laptops with Symantec Endpoint Protection (SEP).

Besides a managed Anti-virus software and Anti-Spyware product, SEP also provides several lines of defence through its managed Intrusion Prevention System and Firewall. Furthermore, it provides Application and Device Control. All these features are instrumental in supporting the governance of ICT policies.

Moreover, SEP prevents any workstation from connecting to more than one network simultaneously; thus eliminating the risk of network bridging.

This software is updated automatically by MITA.

Although MITA is responsible for providing all the necessary support, maintenance and updates with reference to SEP, the NAO recommends that the Medicines Authority requests a periodic report (i.e. every six months) from MITA, to verify that all computers within the Medicines Authority are being updated with the latest definitions. There may be instances whereby either because a computer is disconnected from the network or SEP is not functioning properly, the updates are not installed on a particular computer. The Medicines Authority should be in a position to periodically ensure that this is not occurring.

Furthermore, the NAO recommends that the Medicines Authority requests a quarterly report from MITA, that would indicate which computers were infected with malware and if the malware was removed or not.. This report would help the Authority identify and take any necessary actions needed in the event that the same computers are being affected by malware. In this scenario, the Medicines Authority should educate the users and take the necessary measures to prevent similar instances, as this might pose a risk to the network infrastructure within the Medicines Authority.

4.2 Windows Server Update Services

As part of the support being provided by MITA, the Microsoft Operating Systems and Microsoft Software applications being used by the Medicines Authority are automatically updated through Windows Server Update Services (WSUS). WSUS is a locally managed

system that works with the public Microsoft Update website to give system administrators more control by providing a software update service for Microsoft Windows Operating Systems and other Microsoft Software applications. By using WSUS, MITA manages the distribution of Microsoft hotfixes and patches released through Automatic Updates to Medicines Authority's computers.

Although as explained in the preceding paragraph, MITA is responsible for the distribution of hotfixes and patches to Microsoft Operating Systems and Microsoft Software applications to address identified vulnerabilities, the NAO recommends that the Medicines Authority requests a periodic report (i.e. every six months) from MITA, so as to confirm that all computers within the Medicines Authority are being updated accordingly. The report should include the workstation name and a list of all the missing patches or hotfixes linked to the respective workstation. In return, the Medicines Authority must identify these workstations and ensure that all the missing patches and hotfixes are installed. Furthermore, if the same workstations were included in the previous periodic reports, the Medicines Authority should check whether the workstation is connected to the network or needs to be reconfigured to ensure that all the updates are downloaded automatically through WSUS.

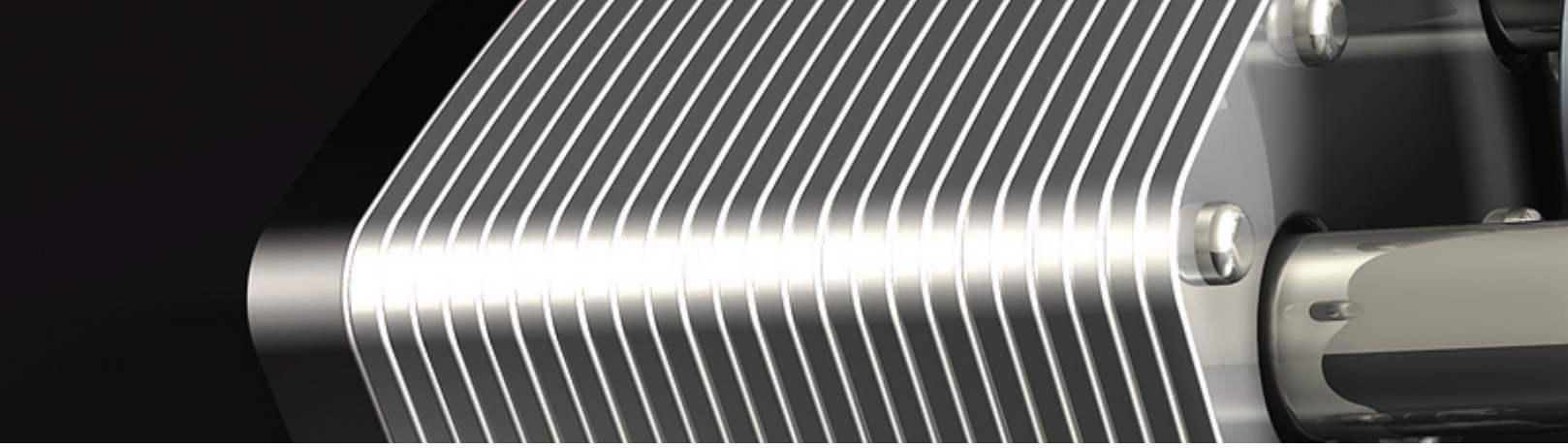
4.3 Electronic mail, Internet Services and Wi-Fi facilities

4.3.1 Electronic Mail & Internet Services

The NAO considers E-mail and Internet Services as mission critical services and principal vehicles for electronic communications both within the Medicines Authority and within external entities.

Today, E-mail is an indispensable office automation system that facilitates the exchange of information, speeds up the decision-making processes, reduces paperwork, increases productivity, reduces communication costs and ensures better delivery of services.

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



Furthermore, NAO noted that the Medicines Authority have also issued circular MA3/10 to its employees about electronic communication highlighting the E-mail Etiquette and the Restrictions on use of E-mail and Internet services. This circular also instructs all employees to use E-Mail signatures provided that the official Medicines Authority template is used.

NAO observed that all Medicines Authority's employees were provided with a government E-mail and Internet account. The personal use of E-mail is discouraged and only allowed in exceptional cases and provided that this does not interfere with the performance of the Medicines Authority's employees and does not compromise the Authority's integrity or image.

Similarly, all Medicines Authority's employees were provided with an internet account. NAO noted that the Medicines Authority holds all its employees responsible and accountable for their Internet activities. Even though an adequate filtering technology is being used by MITA, to prevent access to illegal material, every employee should ensure that his/her account remains secure. Employees are thus responsible for safeguarding their passwords and must not use someone else's password.

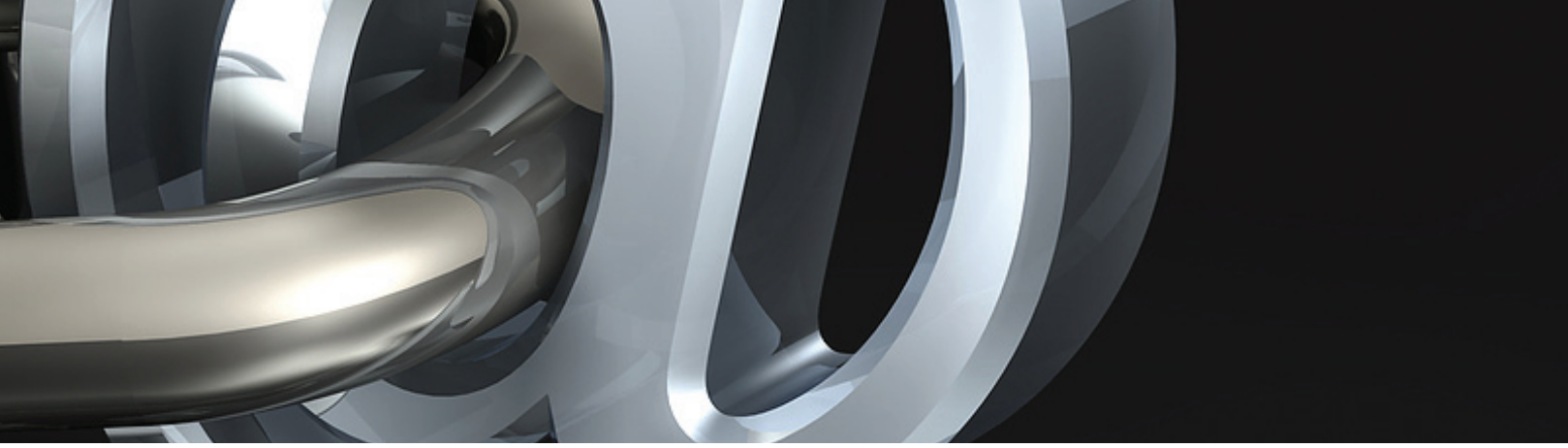
MITA as a service provider, maintains the right to monitor the volume of Internet and network traffic, together with the Internet sites visited by a particular user within the Medicines Authority. The specific content of any transaction will not be monitored unless there is a suspicion of improper use.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

NAO suggests that the Medicines Authority should periodically remind its employees about the salient points highlighted in the E-mail and Internet services directive especially the restrictions on use of E-mail and Internet services as reproduced in **Appendix C**.

4.3.2 Wi-Fi facilities

The Medicines Authority does not have any wireless connectivity anywhere in its building.

In this regard, NAO recommends that if a Wi-Fi facility is implemented the Medicines Authority adopts the Government's Policy in this regard entitled GMICT Policy P 0047:2007 Wireless.



4.4 Physical Security

4.4.1 Stored Documents

Although the Medicines Authority encourages all information passed on to it, including the data it receives from drug manufacturers, to be sent in electronic format it still has a very large amount of paper documents that needs to retain.

The Medicines Authority has three different lock-up rooms storing both the manual paper documents and the CD's/DVD's. Although this information is not classified as sensitive information these documents are generally commercially confidential in their nature.

The NAO observed that all documents are carefully labelled and stored in such a way that they can easily be found. NAO also noted that each of the three rooms storing these documents is equipped with smoke detectors. Furthermore, NAO noted that although fire extinguishers and fire hoses are available in various points throughout the building no fire extinguisher is available in these three rooms.

Although NAO realises that such information can be recollected in case of a disaster, NAO suggests that the Medicines Authority explores the possibility of such information being inputted by the holder directly into the Medicines Authority's IT system avoiding the dependence on manual paper documents.

NAO also noted that given its surroundings and past occurrences the Medicines Authority's buildings may be more susceptible to vermin and observed that all three storage rooms are equipped with pest control appliances so as to mitigate this risk. NAO recommends that the Medicines Authority keeps monitoring this risk and if need be adopts other pest control measures in addition to the existent ones.

Since paper begins to turn yellow and break down as it ages, NAO recommends that proper procedures are devised and followed to ensure that documents remain readable and can be handled while aging. In this regard, NAO recommends that:

- The documents are stored in a stable environment and adequate measures are taken to protect the stored documents from ultraviolet light (exposure to light will cause the documents to deteriorate over time), air pollutants, temperature and humidity levels.

Chapter 4

Protection of Information Assets

- Where appropriate data loggers are installed so as to monitor the temperature and humidity levels in every room. Humidity can cause yellowing, paper rot and/or mildew. Thus climate control helps keep their storage environment dry.

- There is a Records Management system in place, so as to keep track of all the documents stored in these rooms.

4.4.2 Servers

The Medicines Authority's servers are located at MITA. MITA's server room is protected via an aspirating smoke detection system with aragonite gas release. Access to the server room is restricted to authorised personnel through controlled access using electronic access cards and biometrics.

4.4.3 Buildings

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

- A Closed-Circuit Television (CCTV) system which monitors entry and exit to the building and Medicines Authority's offices.

- A visitor's policy is in place whereby the receptionist ensures that visitor particulars are logged and a tag is given to all visitors. Furthermore, the receptionist ensures that all visitors are accompanied by Medicines Authority's personnel. Visitors are also required to sign again when leaving the premises. Medicines Authority has also issued an SOP in this regard namely SS002/01.

- Smoke detectors are installed throughout the building and inspected and tested regularly by the supplier.

- Fire extinguishers and fire hoses are available at various points throughout the building. Fire extinguishers are also inspected on a regular basis. Although the maintenance of the extinguishers is the responsibility of the landlord, this is done through an approved supplier (FSE Fire and Security Engineering). Fire extinguishers are serviced and maintained in accordance with the recommendations and frequencies of BS 5306 Part 3 and refilled when required to BS6643 Part 1 and future amendments. All extinguishers were serviced in December 2011 and are due for maintenance in December 2012.

- An electronic tag is needed to open the Medicines Authority's main door.
- The network equipment is monitored on a 24x7 basis by MITA and the network cabinet is equipped with a UPS
- A backup generator is available.
- Document Storage rooms and the network room are kept locked at all times and accessed by a limited number of staff.

4.4.4 CCTV

The Medicines Authority's premises are monitored by a CCTV system. This system however is owned and monitored by the building's landlord. Cameras are installed at strategic points within the building and focusing on the main door of the Authority, the main door of the building and a 360 degree camera in the corridor leading to the building's lifts. Signage indicating that a CCTV camera is operational are in place throughout these areas.

The Medicines Authority has access to CCTV recordings upon request by the Authority's CEO. CCTV recordings are retained for seven days by the landlord.

NAO suggests that the Medicines Authority ensures that the landlord maintains the CCTV system and that footage is clear enough and made available for possible future playback. Furthermore, the Medicines Authority should ensure that access to live and recorded images are restricted to authorised users only.

Chapter 5

Risk Management, Business Continuity and Disaster Recovery

The Medicines Authority has discussed risk management, business continuity and disaster recovery and compiled a Risk Register. The Risk Register lists down the risks identified and categorises them in four categories namely External Risks, People Risks and Operations and Financial Risks. This document also identifies an owner and rates the possibility and impact of each risk. Furthermore, it identifies the controls in place and the actions to be taken so as to mitigate each risk listed.

The NAO has however observed that the Medicines Authority does not have a formally documented business continuity and disaster recovery plan. Notwithstanding the latter, the NAO noted that Medicines Authority's IT systems are hosted on servers residing at MITA's consolidated environment and notes that, MITA has implemented measures so as to mitigate the risks involved in case of a total failure of Medicines Authority's systems. Furthermore, all the backup tapes are being stored offsite by MITA.

The NAO notes that since the services can be accessed from any premises connected to the Government Network (MAGNET), in case the premises becomes unavailable, the Authority can operate from an alternative site connected to MAGNET.

The NAO suggests that the Medicines Authority compiles and issues a Business Continuity Plan that includes a Disaster Recovery Plan.

5.1 Business Impact Analysis

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

The NAO notes that the Medicines Authority has compiled a Risk Register classifying the impact of identified risks as High, Medium and Low. Following such a good initiative the NAO recommends that the Medicines Authority lists and reviews its critical and non critical functions. For each critical function, the Medicines Authority should then determine the:

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

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

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

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

- The technical requirements for recovery of the critical function.

5.2 Risk Assessment Exercise

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

NAO recommends that the Medicines Authority reviews the Risk Register compiled and ensures that this register takes into account all types of threats that can impact the Medicines Authority's business. Fires, floods, hurricanes, acts of terrorism/sabotage, hardware/software failures, virus attacks, cyber crimes and internal exploits are all examples of the types of threats that are to be analysed assigning a probability assessment value to each.

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

Chapter 5

Risk Management, Business Continuity and Disaster Recovery

5.3 Business Continuity and Disaster Recovery Plans

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

The Business Continuity Plan should:

- Include a list of essential hardware, a list of essential software and a list of essential information;
- State whether the Authority has an alternate site from which to resume operations;
- Preferably include details of manual processes that could temporarily maintain operational functionality for each business process in the event of a total IT system collapse;
- Include a Disaster Recovery Plan that amongst others lists the access rights granted following a restore;
- Include a restoration plan that details how to return operations to normality whether in a restored or in a new facility;
- Identify which resources will be available in a contingency stage and the order in which they will be recovered;
- Identify the key persons responsible for each function in the plan;
- Identify the methods of communication among the key persons, support staff and employees;
- Be documented and written in simple language and understandable to all;
- Be periodically tested;
- Be periodically updated so as to ensure it is kept current;
- Be stored in hard-copy and soft-copy format both on-site and off-site; and
- Be distributed to members of staff, Head of Sections etc.

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

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

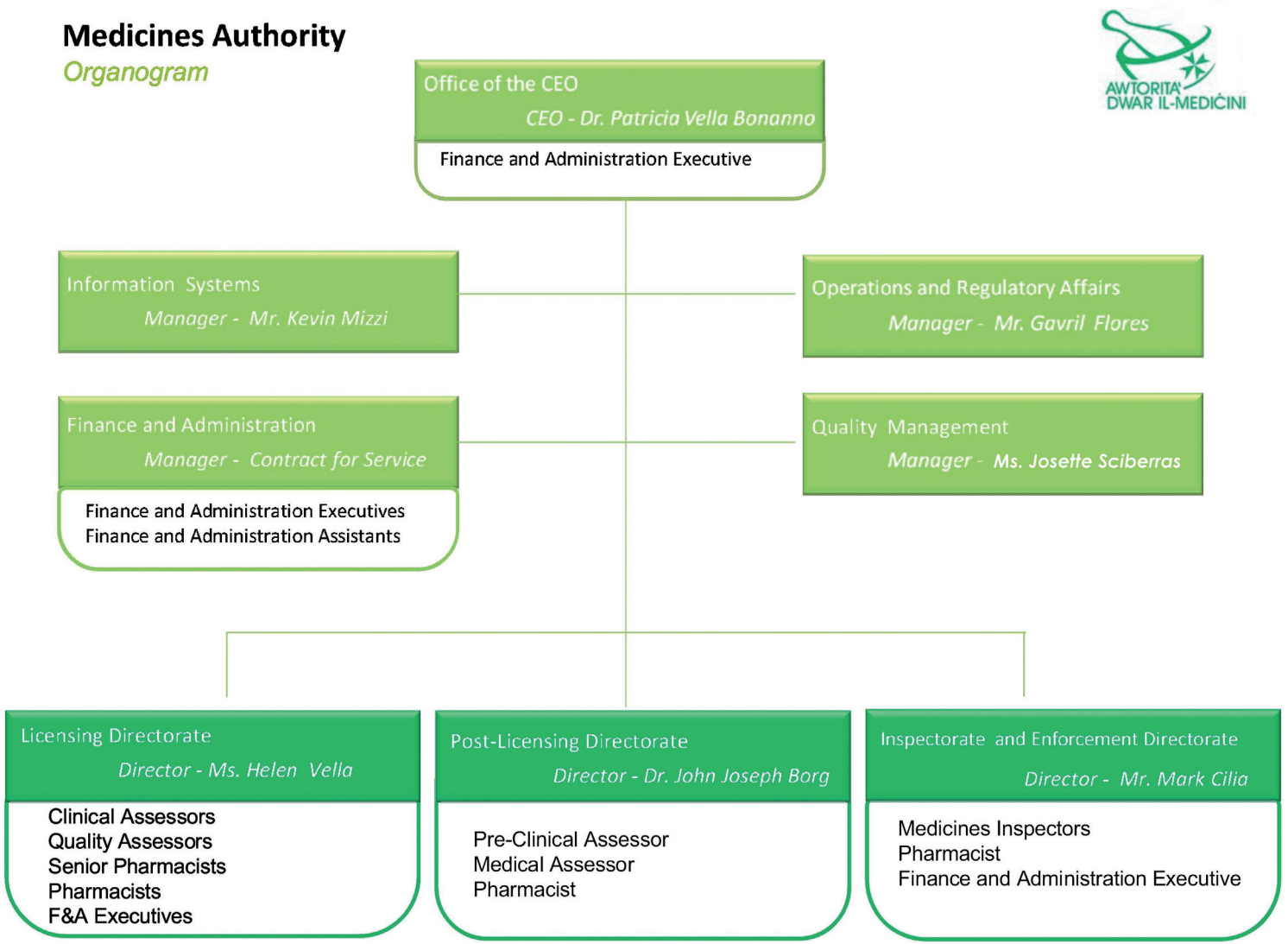
Chapter 6
Management Comments

The following comments were submitted by the Medicines Authority by way of management comments.

- The maintenance agreements are being updated and will soon be finalised;
- To mitigate the risk of a one-person department, the Authority published all relevant documentation on the intranet. In case the IS Manager is not available, the Operations Manager or an admin staff member can phone the relevant entity for help;
- Since no servers are housed within the computer room, the air-conditioning is turned off during the winter months to save on utility costs;
- Hardware inventory – the "server" asset item is referring to the server and networking cabinets. The PC Inventory includes the inventory number of the PC and physical location. It does not indicate any "registrations";
- The structured cabling is manageable as it is currently set up. It will be upgraded when a revamp to the network infrastructure will be carried out;
- A key log is already in place for all rooms within the Authority. This log is also used when accessing the computer room;
- MDIS does not support an authentication mechanism. Therefore the recommendation about the MDIS username/password is not applicable;
- The recommendations about the intranet which are applicable are already in place;
- Although the SEP software indicates the latest definition updates, the Medicines Authority can submit a request to MITA for a periodic report about definitions and infections;
- The Windows operating system does indicate the hot fixes installed on PCs through the Add/Remove Programs feature. However the Authority can request a report from MITA;
- A fire extinguisher is available at the entrance of all documentation stores;
- The process cited in section 2.4.2 is a software development lifecycle process. The latter is usually used for applications developed from the ground up. This is not the case with the new website;
- The Medicines Authority always had business continuity measures in place however they were not documented. A Business Continuity Plan is currently being written which includes an alternative site at the offices of the Superintendent of Public Health.


AWTORITA' DWA'R MEDIĊINI

Appendix A – Organisation Chart



Appendix B – CoBit Controls

CoBit defines IT activities in a generic process model within four domains . These domains[10] are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate as depicted in Figure 8. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

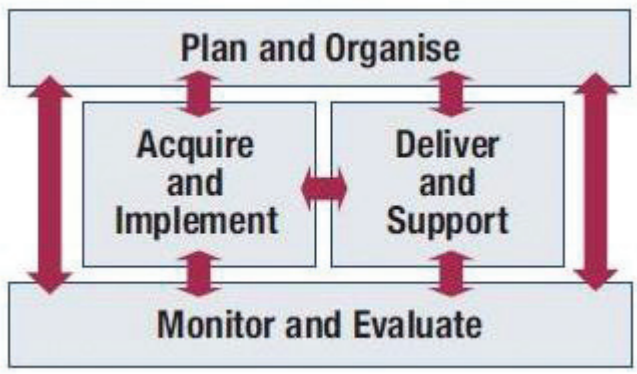


Figure 8: The four integrated domains of CoBit

Plan and Organise

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

Define a Strategic IT Plan

IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and 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.

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

Appendices

Appendix B – Cont

Assess and Manage IT Risks

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

Acquire and Implement

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

Manage Changes

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

Install and Accredit Solutions and Changes

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

Deliver and Support

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

Appendix B – Cont

Define and Manage Service Levels

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

Manage Third-party Services

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

Ensure Continuous Service

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

Ensure Systems Security

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

Manage the Physical Environment

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

Appendices

Appendix B – Cont

Manage Operations

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

Monitor and Evaluate

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

Provide IT Governance

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

Appendix C – Restrictions on the use of Electronic Mail and Internet Services[11]

Restrictions on the use of E-mail services

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

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

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

Appendices

Appendix C – Cont

Restrictions on the use of Internet services

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

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

Recent NAO Publications

NAO Audit Reports

February 2011	Performance Audit: Renewable Energy in Malta Follow-up
March 2011	Performance Audit: Road Surface Repairs on the Arterial and Distributor Road Network
April 2011	Performance Audit: Achieving a Healthier Nutrition Environment in Schools
May 2011	Enemalta Corporation Tender for Generating Capacity (Supplementary Investigation)
June 2011	Performance Audit: Flexible Work Arrangements for Public Employees
July 2011	Performance Audit: Dealing with Asylum Applications
October 2011	Information Technology Audit: Inland Revenue Department
November 2011	ARMS Ltd. – Setting Up and Operations
November 2011	Members of Parliament Honoraria
December 2011	Annual Audit Report of the Auditor General – Public Accounts 2010
February 2012	Performance Audit: Safeguarding Malta's Groundwater
March 2012	Performance Audit: Employment Opportunities for Registered Disabled Persons
April 2012	Information Technology Audit: Heritage Malta
April 2012	Performance Audit: Contract Management Capabilities across Local Councils
May 2012	Performance Audit: An Analysis of the Pharmacy Of Your Choice Scheme
June 2012	Vehicle Emissions Control Schemes – Follow-up
June 2012	Public Broadcasting Services Extended Public Service Obligation
July 2012	University of Malta Concession of parts of University House to the Kunsill Studenti Universitarji

NAO Work and Activities Report

January 2012	Work and Activities of the National Audit Office 2011