N A O
National Audit Office
MALTA

Information Technology Audit:
Malta Industrial Parks Ltd

November 2020

Information Technology Audit

Malta Industrial Parks Ltd*

Report by the Auditor General
November 2020

* With effect from 3rd November 2020, following a rebranding exercise, Malta Industrial Parks Ltd is officially INDIS Malta Ltd.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

BCP	Business Continuity Plan
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CoBit	Control Objectives for Information and related Technology
DoS	Denial of Service
DRP	Disaster Recovery Plan
FSS	Final Settlement System
GDPR	General Data Protection Regulation
GIS	Geographic Information System
GMICT	Government of Malta Information and Communication Technology
HR	Human Resources
ICT	Information and Communications Technology
IT	Information Technology
LAN	Local Area Network
MAGNET	Malta Government Network
MIP	Malta Industrial Parks Ltd
MITA	Malta Information Technology Agency
NAO	National Audit Office
NAS	Network Attached Storage
PC	Personal Computer
Prince2	PRojects IN Controlled Environments
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network

Executive Summary

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

Key Findings and Recommendations

Chapter Two deals with the IT management perspective and analyses the procedures and the way in which information communications technology (ICT) resources are managed at the MIP. The following are the main findings and recommendations included in the above-mentioned chapter:

a. **ICT Strategy** – The National Audit Office (NAO) was informed that the MIP did not have a formally documented long-term ICT strategy however it had 6 monthly IT plans documenting all the work being undertaken to address the ICT needs of the organisation. The NAO recommended that such an ICT strategy is drafted which would prioritise planned ICT investments and link them with the overall MIP business strategy.

b. **ICT Budgeting** – The NAO noted that a minimal percentage of this budget catered for ICT capital expenditure but given that the MIP had invested heavily in setting up new ICT infrastructure in its B'Kara building in 2019, the 2020 ICT budget was primarily allocated for the maintenance of the above ICT infrastructure. The NAO recommended that the recurrent ICT expenditure is reviewed regularly to identify any possible savings related to unutilised ICT resources which carry annual fees.

c. **ICT Hardware Procurement** – The NAO noted that the Chief Financial Officer (CFO) assessed the IT hardware needs and procured goods or services using a tendering or quotations process, however there were instances where the MIP opted for procurement by direct order. The NAO recommended that senior management ensures that IT hardware needs are pre-empted with careful planning and procurement regulations are adhered to when purchasing the required hardware.

d. **Procurement of software applications** – The NAO noted that in 2012 the MIP procured an Integrated Property Management Solution which was customised for MIP's needs. Furthermore, the MIP purchased a number of off-the shelf software packages. The NAO recommended that the MIP formulates a 3-year plan of all its ICT software and infrastructure needs. This plan shall include all significant ICT expenditure including related cost benefit analysis. Through this plan the MIP would lessen the risks associated with adopting a fragmented approach with little integration between existing systems.

e. **Hardware Disposal** – When reviewing the MIP's disposal procedure for IT hardware which was either obsolete or beyond economical repair, the NAO was informed that hard drive/s were removed and the remaining equipment was disposed of accordingly. The NAO was also informed that in the case of laptops, all data and software stored in the related hard disk was deleted and the device was retained by the original user. The NAO recommended that a board is setup to decide which hardware is targeted for disposal and submit a related report to Senior Management.

f. **IT Asset Management** – The NAO noted that the MIP had a hardware inventory that included all PCs; however, such inventory did not include a list of other IT network infrastructure such as network switches. The MIP however provided a list of all the network equipment before the conclusion of this audit. The NAO suggested that the MIP amalgamates the two hardware inventory lists into one list.

The following are the main findings and recommendations detailed in Chapter Three, which includes a review of the IT applications, website and social media used by the MIP:

a. **Integrated Property Management System** – In 2012, the MIP which was then administered by Malta Enterprise invested in a be-spoke integrated property management software system. This application was procured from a local supplier. The NAO noted that:

- this system was procured with GIS capabilities however the MIP was not making use of this functionality.

- the contract signed in 2012 with the supplier of this system still referred to Malta Enterprise / Malta Industrial Parks Ltd and had an initial term of three years which was to be renewed automatically by one year, unless either party had any objection/s.

- the annual maintenance fee listed on the contract was considerably higher than the amount budgeted for this system in the IT budget for the year 2020. The MIP explained that the given that some of the deliverables listed in the original contract were not delivered, the value of the annual maintenance fee was reduced accordingly. The NAO however noted that there was no written agreement reflecting this change in fees.

The NAO recommended that the amended contract lists the MIP's new office address, the current revised annual maintenance fees. The NAO suggests that all contract renewals or changes are made in writing. The NAO also recommended that the MIP makes full use of this system and ensures that this core system continues to reflect MIP's business needs to avoid having multiple systems with multiple databases.

b. **MIP Website** – The NAO noted that a new MIP web site was under construction. The current MIP website was not fully compliant with the Government Website Standards and the *Terms and Conditions* page of the MIP website, still bared the old office address of the MIP at Pieta. Furthermore, the *Tenders* page was not available in the Maltese language and loaded an *Internal Server Error* when accessed. The NAO therefore recommended that the MIP ensures that the above shortcomings are addressed.

Chapter Four of this report covers the controls related to ICT operations and security at the MIP. The following is a list of the key findings and recommendations included in the above-mentioned chapter of this IT audit report:

a. **Anti-virus** – The NAO was given a report listing all the computers on MIPs network and stating which anti-virus was installed on each machine however this report did not indicate whether all PCs were updated with the latest anti-virus definitions. The NAO recommended that the MIP ensures that all its computers are installed with a reputable anti-virus software which is updated automatically with the latest anti-virus definitions. Furthermore, the NAO recommended that the MIP issues quarterly reports that would indicate which computers were infected with malware and whether such malware was removed or not. The reports should also indicate the date of the last update of the anti-virus definitions on each PC.

b. **Patch Management** – The NAO noted that all the PC's at MIP were running Microsoft Windows 10, except 5 PCs which were running Windows 8.1 and 11 PCs which were running Windows 7. The NAO observed that patch management was not updated on all PC's with 7 different version of Windows 10 installed. The NAO recommended that the MIP issues a quarterly report to ensure that all its PCs were updated with the latest operating system patches. Furthermore, the NAO recommends that all PCs are configured to automatically download and install product updates through the Microsoft Windows Update tool.

c. **Backups** – The NAO was informed that a restore of the backup files was conducted just a month before (on the 24th March) however did not see any documentation that determined if this task was a complete restore of MIP data or a test restore of particular backup files. Whilst the NAO commends the off-site backup system at the MIP, it is suggested that the MIP ensures the integrity of data by conducting periodic restores which are signed off by the users, to certify that these restores were successful.

d. **Wide Area Network (WAN)** – The NAO noted that the MIP was connected to the Go plc infrastructure as their primary internet connection and had no back-up connection. The NAO was informed that should this single Internet connection fail, the MIP staff would opt to continue its operations remotely.

The following is a list of the key findings and recommendations included in this Chapter Five which deals with IT risk management:

a. **IT Business Continuity Plan** – During the course of this audit, the NAO observed that the MIP did not have a formalised IT business continuity plan (BCP), however the MIP provided NAO with a related document drafted by their third party contractor for ICT services towards the end of the audit.

b. **IT Security Awareness Training** – The NAO noted that as detailed in Section 2.8 of this report, in 2018 the MIP had organised an Information Security Awareness course for all its employees. The NAO recommended that Information Security Awareness training is given to all new employees as part of their induction training.

Chapter 1

Overview

This chapter provides background information about the audit. It also includes the audit scope and objectives and describes the methodology used in attaining them.

1.1 Background

IT is fundamental to the operations of government organisations. Technology is embedded in most business processes, and it is increasingly becoming more critical because of the ever-growing expectations of the public, demanding a better and quicker service.

The MIP is responsible for the administration of the government-owned industrial parks and related facilities around Malta and Gozo, as well as supporting and promoting their further development. The MIP also manages the largest industrial property portfolio in Malta, spread across a number of industrial zones around the Maltese islands, which also includes those dedicated to specific sectors.

The industrial estates were placed under the responsibility of the MIP by means of Legal Notices issued in 1997 and 2003. The MIP entered into a contract with Government in order to administer Government-owned parks up to 2040, which can also be extended for additional periods. The MIP had a number of lease agreements and contracts of temporary emphyteutic concessions with tenants, both local and foreign investors, operating from the industrial estates.

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

1.2 Organisation Structure

The MIP operates from its head office situated in 88, Msida Valley Road B'Kara. The MIP is composed of three operational departments (namely the Industrial Projects, Technical Project Support and Facilities and the Property Management Solutions) and two administrative departments (namely the Human Resources (HR) and the Finance). All 5 departments are headed by a Chief Officer who are answerable to a Chief Executive Officer (CEO).

Furthermore, the MIP administers the Safi Aviation Park located close to the Malta International Airport where it provides secure airside facilities for the aviation industry. The MIP has an office at the Safi Aviation park that is administered by one employee.

The MIP is also responsible for the administration of the Gozo Innovation hub located at the outskirts of the Xewkija Industrial Estate in Gozo. The hub is a unique campus style development that is planned to accommodate various operations in the knowledge-based economy. It was inaugurated at the end of 2019 and is not yet fully operational. The MIP has an office at the Gozo Innovation hub that is administered by one employee.

The Organogram of the MIP is included in Annex A.

1.3 Workforce Distribution and family friendly measures

The total workforce of the MIP was made up of 71 employees which were distributed as shown in the Figure 1.

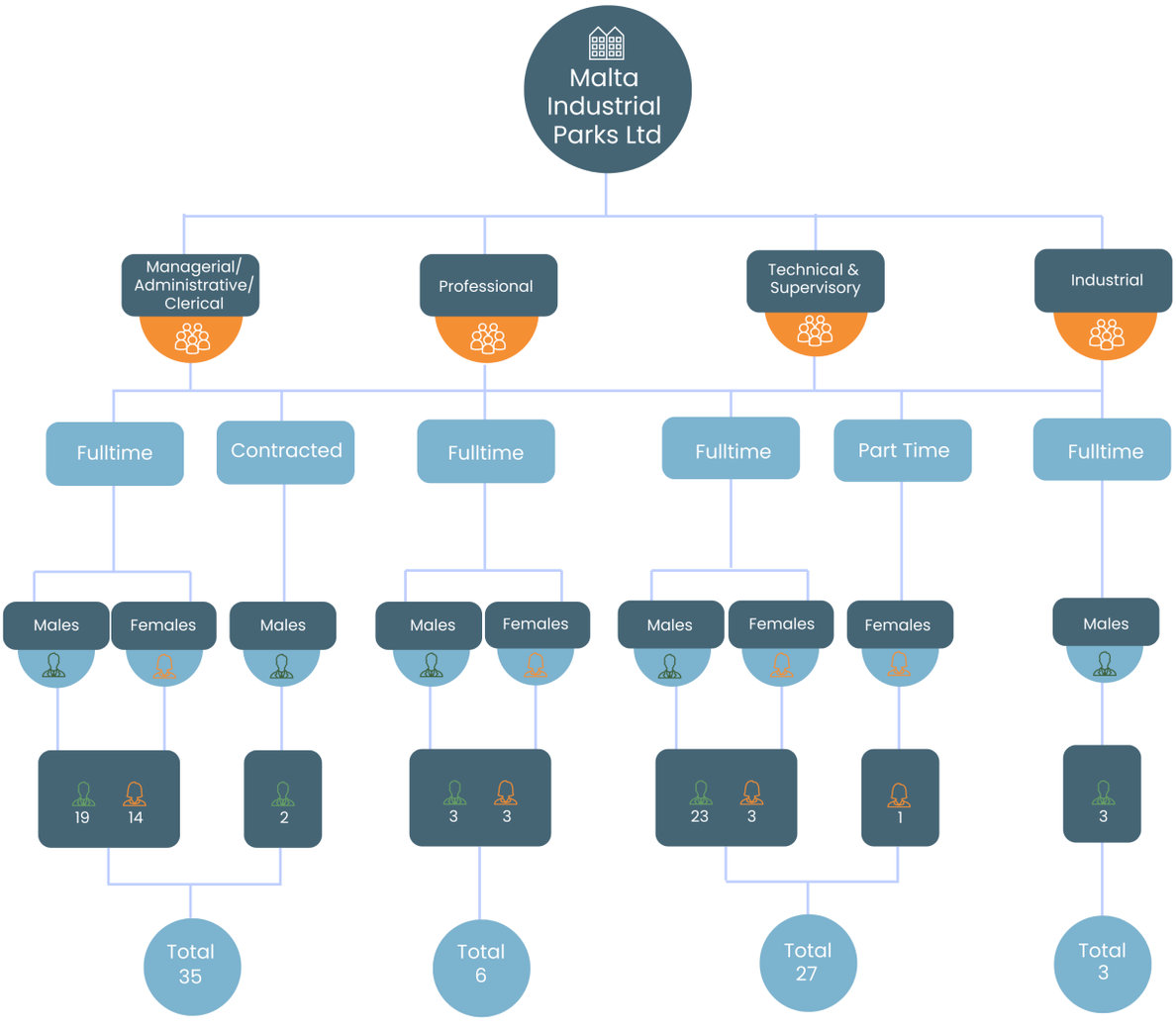


Figure 1: Workforce Distribution

The majority of MIP employees were equipped with laptops whilst all employees had access to printers and could make use of Virtual Private Network (VPN) connections providing access to all systems as if employees were at the office. Although the MIP originally did not have any of its employees tele-working, the impact of COVID-19 dictated that a number of employees had to work from home in line with health recommendations. The latter required documentation to be taken home. Figure 2 shows the number of employees that made use of family friendly measures.

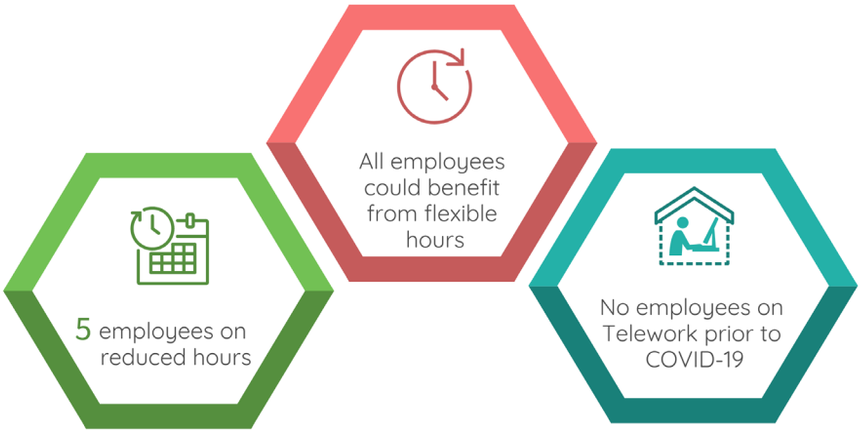


Figure 2: Employees using family friendly measures

1.4 Legislation

The MIP is designated as the competent authority for the purposes of article 2 of the Commissioner of Land Ordinance Chapter 169[1].

The rights and liabilities in respect of the land specified in the First Schedule[2] of this act, where, with effect from the dates specified in the said Schedule, exercised by the MIP.

[1] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12698&l=1
[2] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=9525&l=1

1.5 Information Communications and Technology at the MIP

The ICT infrastructure at the MIP was made up of the below listed hardware, software and network equipment.

1.5.1 Hardware

The ICT infrastructure at the MIP consisted of the hardware listed in Table 1.

Item	Amount
Personal Computers	10
Laptops	50
Scanners	2
Stand-alone Printers	5
Multi-Functional Printers	5
Projectors	1
Monitors	52
Plotters	1
TVs	5

Table 1: Hardware at the MIP

1.5.2 Software

The MIP processes, stores and maintains a considerable amount of data as part of its daily functions. This data is processed using office automation software applications and the below listed software:

- Integrated Property Management Solution based on LEMIS – a system developed locally for the MIP. This system is used to keep an electronic record of all Government property;
- Infor SunSystems Query and Analysis – is a reporting tool that is used to analyse data, create reports and identify trends, patterns and/or exceptions;
- Dakar – provides payroll processing including the management of leave and submission of Final Settlement System (FSS) returns as required by the current legislation;
- AutoCAD – a computer aided software drafting program used to create and amend blueprints for buildings;
- N4ce – a survey processing package with modelling functionality used by engineers and surveyors;
- Geographic Information System (GIS) – a geographical information system that provides the ability to capture and analyse spatial and geographical data;

- Auto Turn – used to analyse road and site design projects including intersections, roundabouts and clearances; and

- Auto Park – used to design parking layouts.

The NAO noted that the MIP only had one custom built software (Integrated Property Management Solution) and used multiple off-the shelf packages as listed above.

1.5.3 Network

The MIP was connected to the Go plc infrastructure as their primary internet connection. The NAO noted that the MIP had no back-up wide area network (WAN) connection.

The NAO was informed that data saved within the personal folders of each employee and saved on the server, was backed up on OneDrive that forms part of Microsoft Office 365 suite.

1.5.4 Servers and Data Storage Equipment

The MIP had one physical server and a Network Attached Storage (NAS) device that was installed in a dedicated server room. The management of the above infrastructure was contracted out to a third-party supplier by the CEO. Supplier management was conducted by the CFO.

Furthermore, the MIP made use of cloud services for hosting of core systems and data storage purposes.

1.5.5 Electronic Mail

The MIP made use of the Microsoft Office 365 and all mailboxes were synchronised with the Office 365 cloud.

1.6 Audit Scope and Objectives

The scope of this IT audit was to analyse the IT and Information Systems used within the MIP, to determine whether the MIP has the necessary controls to maintain data integrity, safeguard assets, allow organisational goals to be achieved effectively and to ensure the efficient use of the Government IT related resources.

The audit report identified any potential risks and made the necessary recommendation to mitigate those risks. However, given that the scope of this audit was to carry out an IT audit, the review of the selected software applications should not be considered as a detailed Information Systems audit. Such audits would normally be carried out as a standalone review for a particular system.

During this IT audit, the NAO reviewed the level of controls in place related to IT network infrastructure, IT security and data backups. In this regard, the objectives of this report were to:

- document all the information collected from the various key stakeholders and officials;
- summarise the documentation collected and elicit the area/s of concern;
- determine whether the MIP's IT setup operates effectively, efficiently and economically;
- list all the findings and identify any potential risks; and
- list all the recommendations to mitigate those risks.

1.7 Audit Methodology

The IT audit was divided into three different stages:

- Initially, a pre-audit questionnaire was sent to the MIP to gather the necessary information on the auditee prior to undertaking an on-site audit. The aim of the questionnaire was designed to familiarise the NAO audit team with MIP and its setup. Given that this audit was conducted during the Covid-19 pandemic the audit team relied heavily on documentation provided by the auditee and on-site audit visits had to be kept to a minimum.
- The NAO then went through MIP's overall strategic direction, objectives, internal structures, functions and processes to gain a comprehensive understanding of MIP and its environment.
- The third stage examined how the IT applications are being used to achieve their objectives.

The audit methodology adopted by the NAO was based on the Control Objectives for Information and related Technology (CoBit) set of best practice guidelines which includes a review of Business Continuity and Disaster Recovery measures.

CoBit is a comprehensive set of resources that contains all the information organisations need 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 controls that were considered during this audit are listed in Annex B.

1.8 Structure of the Report

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

- Chapter two deals with the IT management perspective and analyses the procedures and the way in which ICT resources are managed at the MIP.
- Chapter three includes a review of the IT applications, website and social media used by the MIP.
- Chapter four covers the controls related to ICT operations and security at the MIP.
- Chapter five deals with IT Risk Management including Business Continuity and ICT security related training.
- Chapter six lists the management comments and includes the agreed recommendation implementation schedule.

1.9 Acknowledgements

The NAO would like to express its appreciation to all the key stakeholders who were involved in this audit, including the MIP CEO, the CFO and the Head of Risk Management and Internal Audit, for their time and assistance. The NAO commends the proactive approach adopted by the MIP in managing their ICT operations which was evidenced throughout the audit.

Chapter 2

IT Management

This chapter focuses on IT Governance and reviews the way in which ICT resources / services are procured and managed. Furthermore, it reviews the availability of ICT support at MIP as well as the provision of the IT / Security Awareness training being given to MIP employees.

2.1 IT Unit

The NAO noted that up until July, 2019, the MIP used to share a building with another entity which had its own fully-fledged IT unit. This meant that the IT Infrastructure was shared and MIP did not need its own IT personnel. However, in July 2019, the MIP moved to its own premises and since then, the CFO was given the responsibility for ICT operations and the management of ICT maintenance and support provided by third party suppliers.

The NAO observed that the MIP had a service level agreement (SLA) with a third-party supplier to setup, maintain and support IT systems that included servers, networks and telephony. This agreement also covered the maintenance and support of PCs and the setting up and support of Microsoft Windows Operating Systems, Microsoft Office suite of applications and the Microsoft Office 365 platforms.

The NAO noted that the above-mentioned SLA commenced on the 1st May, 2019 for a period of 3 months which could be automatically renewed for an additional 3 months but not exceeding a total of 3 years. The NAO observed that the MIP had a non-disclosure and confidentiality agreement with the same supplier dated 30th April, 2019.

During the course of this audit the MIP issued two separate calls for the recruitment of an IT Executive, however no candidate was selected. The NAO was informed that a third call for applications was to be issued.

The NAO obtained a copy of the job description of this IT Executive which stated that this executive would report to the CFO and his/her job would mainly involve the support and maintenance of IT hardware, telephony and network infrastructure.

Recommendations

The NAO commends the MIP's decision to recruit an IT executive and recommends that the recruited IT Executive assist MIP senior management in the development of a three-year ICT strategy. The ICT Executive would be responsible for the implementation of the tasks mentioned in the ICT strategy in order to achieve the related strategic objectives.

2.2 ICT Strategy

The NAO considers that an ICT strategy is essential more so in entities like the MIP which need to maximise the return on their ICT investments notwithstanding the limited ICT resources available.

During the course of this audit, the NAO was informed that the MIP did not have a formally documented long-term ICT strategy, however it had 6 monthly IT plans documenting all the work being undertaken to address the ICT needs of the organisation. The NAO reviewed these short-term strategies starting from July 2019 until November 2020 and commends the detailed short-term plans within such documents.

Recommendations

The NAO suggests that the MIP formulates a long-term ICT strategy that:

- refers to the ICT and Information Systems projects, and explains how these projects are linked to the MIP business strategy, and how these projects shall be implemented;
- prioritises future ICT investment;
- covers the development being planned in the next three to five years; and
- refers to the logical and physical architecture of the MIP IT systems.

Through this ICT strategy, management can gauge whether ICT investment is assisting the organisation its strategic objectives and can ensure that the ICT investment is not misdirected and draining resources, which could otherwise be deployed differently to the benefit of the organisation. In order to achieve the above, the MIP should ensure that senior management are duly consulted during the drafting of such a strategy both from an input and review perspective.

2.3 ICT Budget

During the course of this audit, the NAO reviewed the actual ICT capital and recurrent expenditure of the MIP.

The NAO also reviewed the percentage of ICT funds being spent on new ICT investment and compared it with the percentage of ICT funds allocated towards ICT support.

The MIP provided their ICT budget for 2020 amounting to €145,600. This budget was split as per Figure 3:

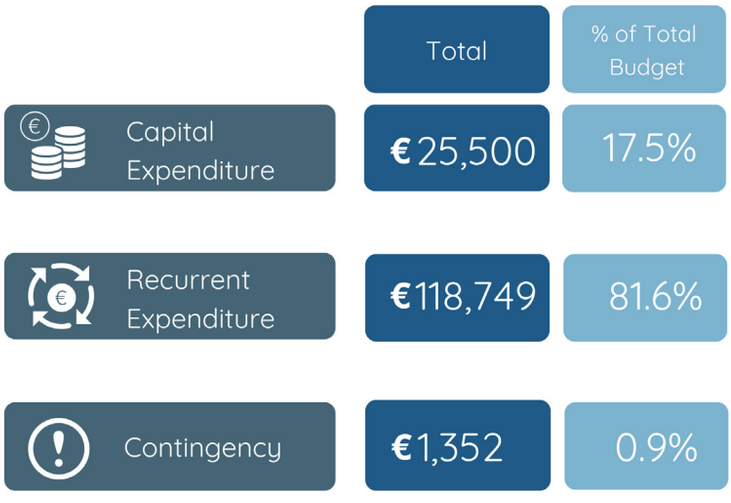


Figure 3: ICT Budget for 2020

The NAO noted that the 2020 allocation for capital expenditure was only 17.5% of the total budget indicating that the no major ICT investment was planned for this year. This is attributed to the fact that in 2019 the MIP had already invested heavily in new ICT infrastructure as part of their move from Malta Enterprise premises to their new offices in B'Kara.

Recommendations

The NAO recommends that the recurrent expenditure is reviewed regularly to identify any possible savings related to unutilised ICT resources which carry annual fees.

2.4 Procurement of Hardware

The NAO reviewed the procurement of ICT hardware at the MIP and analysed how it identified hardware procurement needs and the method of procurement adopted.

The NAO noted that the CFO assessed the IT hardware needs and proceeded with procurement of the goods or services required. The NAO was informed that procurement was done through open procedures (tender or quotations) however there were instances where the MIP opted for procurement by direct order.

Recommendations

The NAO recommends that senior management ensures that IT hardware needs are pre-empted with careful planning and procurement regulations should be adhered to when purchasing the required hardware.

Furthermore, the NAO suggests that MIP's IT hardware needs are assessed by the IT executive being recruited who can determine the best set of specifications for the hardware needed. The IT executive should actively contribute to the process for the evaluation of the tender submissions or quotations received and the preparation of a technical report for the consideration of senior management. This evaluation process would include other stakeholders within MIP management such as the CFO.

2.5 Procurement of Software

The NAO noted that in 2012, the MIP had procured an Integrated Property Management Solution which was customised for MIP's needs. Furthermore, the MIP purchased a number of off-the shelf software packages.

Recommendations

The NAO recommends that the MIP formulates a plan of all its ICT software and infrastructure needs over the next 3 years. This plan shall include all significant ICT expenditure including related cost benefit analysis. Through this plan the MIP will lessen the risks associated with adopting a fragmented approach with little integration between existing systems.

This plan should also include a comparative analysis between the use of cloud services as compared to using locally hosted systems with adequate support services.

2.6 Hardware Disposal

During the course of this audit, the NAO reviewed the procedure adopted by the MIP for the disposal of IT hardware which was either obsolete or beyond economical repair. The NAO was informed that hard drive/s were removed, and the remaining equipment was disposed of accordingly. Moreover, it resulted that in the case of laptops, all data and software was deleted and the device was retained by the original user.

Recommendations

The NAO recommends that an internal board, possibly made up of IT and Admin staff, is setup to decide which hardware is to be disposed of. This board should submit a report listing all the IT equipment to be disposed of, to Senior Management copying the Accounts Section and the person in charge of the hardware inventory. Furthermore, the NAO recommends that such reports should include:

- Date of survey;
- Members on the board of survey;
- Item inventory number;
- Item serial number;
- Item description;
- Reason for disposal (ex. certified beyond economical repair, certified obsolete).

Moreover, the NAO suggests that all hardware that is beyond economical repair or obsolete, is certified in writing. The related certification should then be handed to the board of survey together with the item in question and attached to the board of survey's final disposal report.

The NAO also recommends that the MIP adopts the Government of Malta Information and Communication Technology (GMICT) Desktop Services Procedure (GMICT R 0084:2009)[3] in terms of PC disposal and data wiping, and ensures that data on equipment being disposed of could not be retrieved.

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

2.7 IT Asset Management

The NAO acknowledges that one of the toughest tasks for IT managers and administrators is keeping track of computers, network devices and software applications. However, this is considered to be critical since such information would enable the MIP to keep track of its IT investments and manage these resources efficiently.

The NAO sought to obtain a copy of the IT hardware and software inventory. The NAO noted that the MIP had a hardware inventory that included all PCs however such inventory did not include a list of other IT hardware / network equipment ex. network switches. The MIP however provided a list of all the network equipment before the conclusion of this audit.

Recommendations

The NAO suggests that the MIP amalgamates the two hardware inventory lists into one list. In the case of PCs this inventory should include details such as the type of processor, the hard drive capacity and the amount of RAM installed. These fields will provide a clear picture of the general specifications of MIP's IT hardware and would assist management in assessing suitability of current hardware when planning for new IT systems.

2.8 IT Training

The NAO observed that all MIP employees in 2018 were given an Information Security Awareness course. This course was spread over two half days and included an assessment based on multiple choice questions. All MIP employees successfully completed the course and were provided with certificates. The course covered the key skills and main concepts relating to ICT, computers, devices and software.

Furthermore, the NAO noted that 8 employees attended a Prince2 (PRojects IN Controlled Environments) Foundation and Practioner course in the first half of 2019. Another 2 employees attended such course during 2018. This course provides attendees with the required skills to manage projects including IT projects.

Recommendations

The NAO recommends that the MIP draws up a yearly IT training plan based on the training needs analysis of its employees.

Chapter 3

IT Applications

This Chapter includes a review of a number of software applications currently used at the MIP.

3.1 Integrated Property Management Solution based on LEMIS

In 2012, the MIP which was then administered by Malta Enterprise, invested in a be-spoke integrated Property Management software system. This application was procured from a local supplier. The system was based on the LEMIS software application used by the Lands Departments but customised to MIP's business needs.

Initially, the supplier conducted an in-depth analysis of MIP's business processes prior to configuring the LEMIS databases for the processes adopted at the MIP. Migration of data related to more than 1000 properties and over 1300 lease contractors was carried out. The spoke integrated property management system catered for:

- Property Management;
- Asset Management;
- Property Portfolio Management;
- Property Maintenance Management;
- Contract Management;
- Facilities Management;
- Rent Revenue Collection and management (Receivable and Payable);
- Invoicing and Tax Management;
- Customer Management;
- Multi Property;
- Acquisition and Disposal Management.

The system dealt with property lease renewals and rent reviews in an automated fashion and generated invoices automatically. The system exported the totals of the related financial transactions to MIP's accounting package and had a number of management reports including:

- Master data report which allowed users to extract data related to properties, tenants and leases by selecting the appropriate parameters. Once this data was extracted and exported to Microsoft Excel users could format the data as required.

- Transaction analysis report which was used to extract financial data from the system. Similarly, to the above this data could be exported to Microsoft Excel and formatted as required.

- Revenue report which provided the revenue generated as at the previous year end together with the revenue as at the cut-off date supplied by the user. This report could also be used to carry out in-depth analysis at lease level.

- Tenant ledger history and tenant statement of account which generated a full review of the transactions for a particular tenant. This report was produced in a form which could easily be folded into a letter and sent to the tenant.

- Aged analysis report which was used to analyse debts due by tenants.

- Cash flow projection which was used to view a forecast of revenue that should be generated as at the cut-off date provided by the user.

- Rent reviews report which were used to extract the leases that were up for review within a given date range.

The NAO noted that this system was procured with GIS capabilities, however the MIP was not making use of this functionality.

The NAO reviewed the contract signed with the supplier of this system and noted that this contract still referred to Malta Enterprise / Malta Industrial Parks Ltd. The contract was signed in 2012 with an initial term of three years which was to be renewed automatically by one year, unless either party had any objection/s.

The NAO also noted that the annual maintenance fee listed on the contract was considerably higher than the amount budgeted for this system in the IT budget for the year 2020. It was also unclear whether the MIP was paying annual licence fees for the GIS functionality of this system which it did not use. The MIP explained that this contract was signed upon commencement of this project and never updated. The MIP also stated that the given that some of the deliverables listed in this contract were never delivered, the value of the annual maintenance fee was reduced accordingly. The NAO however, noted that there was no written agreement reflecting the latter change.

Furthermore, the NAO observed that this contract did not include the obligatory General Data Protection Regulation (GDPR) contract clauses. The NAO observed that in January 2019, the MIP had drafted a proposed addendum to this contract so as to make it compliant with GDPR however the supplier never signed this addendum or proposed any changes.

Recommendations

The NAO recommends that, given that the MIP is now totally independent from Malta Enterprise, the contract is amended accordingly. Moreover, the NAO recommends that the amended contract lists MIP's new office address, the current revised annual maintenance fees and include the required GDPR contract clauses. The NAO drew MIP's attention to the fact that all contract renewals or changes need to be made in writing.

The NAO also recommends that the MIP makes full use of this system and ensures that this core system continues to reflect MIP's business needs so as to avoid having multiple systems with multiple databases.

3.2 MIP Website

The MIP had a website with the following Uniform Resource Locator (URL) *www.mip.com.mt* as per Figure 4. This website was hosted on servers administered by the third party contractor who was also in charge of its backup and developed by another local contractor who was also responsible for assisting with all MIP website requirements, including updates, issues and errors. This website has a content management system which was administered by MIP.

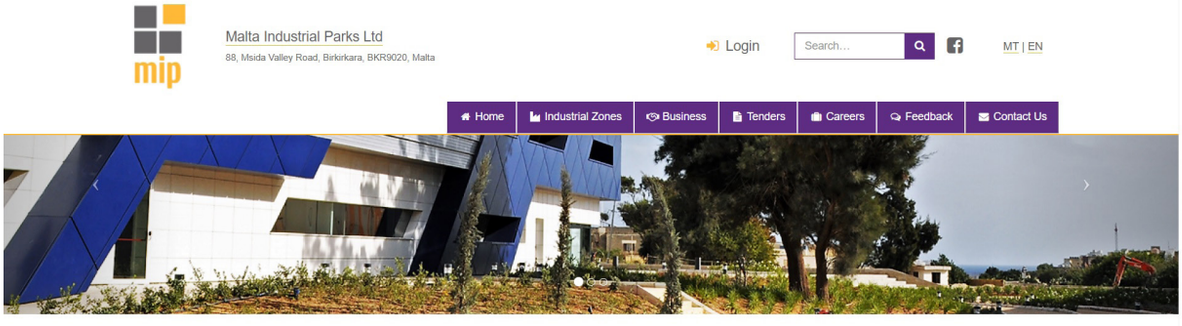


Figure 4: MIP Website

The NAO reviewed this website and noted that it was bi-lingual and optimised for mobile devices. This website could also be used by tenants to pay rents and access their related rental accounts. The NAO however noted that this website was not fully compliant with the Government Website Standards. The NAO also noted that the *Terms and Conditions* page of the MIP website, still bared the old office address of the MIP at Pieta. Furthermore, the *Tenders page* was not available in the Maltese language and was giving an *Internal Server Error* when accessed.

Recommendations

The NAO understands that this website will soon be made redundant and the MIP is designing a new website. The NAO recommends that the MIP ensures that this new website complies with the Government Standards and the guidelines of the National Commission for Persons with Disability and the Foundation for Information Technology Accessibility.

3.3 Social Media

The NAO noted that the MIP had an official Facebook page. This was launched in Q2 2016 and was being maintained by the person in charge of public relations. The NAO noted that this Facebook page was updated just twice in the last year and in both occasions, it was used for recruitment purposes. Finally, the NAO noted that the MIP Facebook page had 288 likes and no rating or reviews.

Recommendations

The NAO recommends that the MIP markets its Facebook page better so as to increase its audience. One way of doing this is by continuously updating this page with tenders and any other notices that are uploaded on the MIP website.

Chapter 4

IT Operations and Security

This chapter analyses the Information Security and evaluates the security measures adopted by the MIP to maintain confidentiality, integrity and availability of data.

4.1 Anti-Virus Software

During the course of this IT audit, the NAO noted that all the MIP's PCs except three, were installed with a reputable anti-virus application, two PCs had no anti-virus installed and another PC had a free basic anti-virus. The NAO also noted that the MIP had no anti-virus on its servers.

The NAO was given a report listing all the computers on MIPs network and stating which anti-virus is installed on each machine however this report did not indicate whether all PCs were updated with the latest anti-virus definitions.

Recommendations

The NAO recommends that the MIP:

a. ensures that all its computers are installed with a reputable anti-virus software which is updated automatically with the latest anti-virus definitions.

b. issues quarterly reports that would indicate:

- which computers were infected with malware and whether such malware was removed or not; and
- the date of the last update of the anti-virus definitions on each PC.

4.2 Patch Management

The NAO noted that all the PC's at the MIP were running Microsoft Windows 10, except 5 PCs which were running Windows 8.1 and 11 PCs which were running Windows 7. The NAO observed that patch management was not updated on all PC's with 7 different versions of Windows 10 installed.

Recommendations

The NAO recommends that the MIP issues a quarterly report to ensure that all its PCs were duly updated with the latest operating system patches. Furthermore, the NAO recommends that all PCs are configured to automatically download and install product updates through the Microsoft Windows update tool.

4.3 Backups, Off-site Storage and Recovery of Data

The NAO observed that most of the MIP data was hosted on a cloud storage and remote backups were done by the cloud service provider. However, the MIP had a server that acted as a document repository. The NAO noted that this server was being mirrored onto a NAS device and backed up remotely to a cloud storage.

The NAO was informed that a restore of the backup files was conducted just a month before (on the 24th March) however no documentation that determined if this restore was a complete restore of MIP data or a test restore of particular backup files was provided.

Recommendations

Whilst the NAO commends the off-site backup system at the MIP, the NAO suggests that the MIP ensures the integrity of data by conducting periodic restores which are signed off by the users, to certify that these restores were successful.

4.4 Internet Services and Electronic Mail

During the course of this IT audit, the NAO noted that the MIP used a cloud-based e-mail system and had one Internet connection with a service provider. The NAO was informed that should this single Internet connection fail, the MIP staff would opt to continue its operations remotely. Furthermore, the NAO observed that the MIP had a user security policy that included a policy on the Internet and e-mail services.

The NAO suggests that the MIP issues periodical reminders to all e-mail and Internet users, highlighting the salient points in the ICT user security policy and the user responsibilities in connection with mailbox maintenance.

4.5 Multi-Function Printers

The NAO noted that the MIP had 5 multi-function printers and 5 stand-alone printers within its offices. The NAO was pleased to observe that these printers were equipped with a secure printing facility whereby documents were not printed until the correct PIN was entered on the operation panel of the machine or the relative printing key fob was swiped. This feature kept printouts of confidential documents from being left unattended. Furthermore, the NAO noted that MIP's senior management had access to real-time activity logs which helped to ensure that there was no misuse of the equipment.

4.6 Wide Area Network

As stated in Section 1.5.3 of this report, the MIP was connected to the Go plc infrastructure as their primary internet connection and had no back-up connection. The NAO was informed that should this single Internet connection fail, the MIP would opt to continue its operations remotely.

4.7 Server Room

During the audit, the NAO also held a site inspection in the MIP's server room and observed that this room was equipped with a fire alarm sensor and an air-conditioning unit. The NAO also noted that access to this room was electronically controlled and the room was tidy with adequate cable management in place. Furthermore, the NAO observed that related fire extinguishers were placed outside the room and these were serviced regularly.

However, the NAO noted that this room was not equipped with a humidity/temperature monitor that sends alerts via e-mail / SMS if it reaches a pre-defined threshold. The NAO communicated the latter with the MIP during the site inspection and the MIP took immediate action to rectify this matter.

Chapter 5

IT Risk Management

This final chapter analyses the management of IT risks within the MIP. The process of IT risk management is designed to reduce or eliminate the risk of certain events happening or having an impact on the IT operations of the organisation. It thus entails identifying, assessing and prioritising risks of different kinds. Furthermore, once the risks are identified the organisation needs to devise a business continuity plan (BCP) to minimise or eliminate the impact of negative events.

During the course of this audit, the NAO observed that the MIP did not have a formalised IT BCP. In order to draw up such a plan, the MIP would need the conduct the related business impact analysis, risk assessment and procedures for business continuity and disaster recovery.

During the concluding phase of this audit, the MIP provided NAO with a document drafted by their third party contractor for ICT services. This document outlined the restoration of IT and telephony services in case of a disaster and provided an estimate of the downtime.

5.1 Business Impact Analysis

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

Recommendations

The business impact analysis process is based upon the information that is collected from key users within all the units at the MIP. The information can be collected using different approaches, such as the questionnaire approach, whereby a detailed questionnaire is circulated to the key users within the MIP. Another alternative is to interview a number of key users. Ultimately, all the information gathered during these interviews or from the questionnaire responses is tabulated and analysed in order to draft a detailed business impact analysis plan and strategy.

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

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

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

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

5.2 Risk Assessment Exercise

The NAO is of the opinion that a cost-effective BCP needs to be part of a structured overall risk management approach, which should include an analysis of business processes and the risks that these processes are exposed to. For example, the entity would need to assess the level of risk (if any) related to the fact that the MIP hosts data on third party cloud storage and that the data residing in the server located at the MIP is replicated on the cloud storage environment.

The NAO noted that the MIP stated that they had done a risk assessment exercise however this was not given to the NAO for review.

Recommendations

The NAO recommends that the MIP identifies and documents its risks, taking into account all types of threats that can impact its business. Fires, floods, acts of terrorism/sabotage, hardware/software failures, connection failures, virus attacks, Denial of Service (DoS) attacks, cyber-crimes and internal exploits are all examples of the types of threats that are to be analysed, assigning a probability assessment value to each. The MIP should then document the probability assessments, and devise alternative solutions identifying the countermeasures that may be deployed to deal with these threats and the potential costs associated with each solution.

5.3 Business Continuity and Disaster Recovery

The primary objective of a BCP is to define the actions required to re-establish the MIP operations in the event that all or part of MIP's ICT systems and infrastructure, have been rendered unusable. The BCP identifies the critical IT application programs, operation systems, networks, personnel, facilities, data files, hardware and timeframes required to assure high availability and system reliability, based on the inputs received from the Business Impact Analysis and Risk Assessment exercise. This plan also defines the roles and responsibilities of the key persons authorised to carry out the related BCP tasks.

As part of the above-mentioned BCP, an entity should develop a disaster recovery plan (DRP) dealing with the process of rebuilding the operations or infrastructure and recovering the entities' business applications following a disaster. The DRP should stipulate the procedures that are to be considered in the event that the IT facilities become inoperative. 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.

Recommendations

In this regard, the MIP should draw up a formal documented BCP and DRP, designed to reduce the impact that disruptions might inflict on the entity's operations. (vide Annex E).

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

Apart from having a DRP, the MIP should ensure that the SLAs it has with its suppliers cater for an adequate and timely maintenance, support and IT business continuity.

5.4 Security Awareness Training

The NAO acknowledges that one of the best ways for an entity to improve information security is by raising awareness and training everyone who interacts with its computer network, systems and information about the most important aspects of information security.

The NAO noted that, as detailed in Section 2.8 of this report, in 2018 the MIP had organised an Information Security Awareness course for all its employees.

Recommendations

The NAO recommends that Information Security Awareness Training is given to all new employees as part of their induction training.

Chapter 6

Management Comments

This audit report was discussed with MIP and comments were as follows:

Chapter 2

a. **IT Unit**: MIP management notes that whilst a third call for the recruitment of an IT executive has been issued and is in process, there has not been much interest and no ideal candidate has been identified.

b. **ICT Strategy**: MIP management notes that MIP has, to date, bi-annual IT plans rather than long term plans as a result of the fact that MIP's experience in this field was limited given that until recently the company's IT needs were serviced by the Malta Enterprise IT Unit. MIP management notes further that MIP is currently working towards a three-year vision, compartmentalised into six-month tranches. In this context it is envisaged that the three-year ICT Strategy documenting MIP's current (Q1 2021) status together with improvements required and an "ideal to have" list will be complete in Q1 2021.

c. **ICT Budgeting**: MIP management notes that recurrent expenditure is high due to the fact MIP services and productivity are all cloud based. Whilst this translates into a significant monthly cost, it also ensures that the latest technology is always available.

d. **ICT Hardware Procurement**: MIP management notes that direct orders are only granted as a last resort as is evidenced by the fact that the recent purchase of laptops was conducted using an open call for tenders.

e. **Procurement of software applications**: MIP management notes that NAO's recommendation is to be tackled as part of the ICT strategy plan.

f. **Hardware Disposal**: MIP management notes NAO's recommendation and is working to ensure that by Q1 2021, an appropriate hardware disposal system will be implemented.

g. **IT Asset Management**: MIP management notes that MIP has implemented software that overviews all the MIP infrastructure including servers, PCs, switches, and access points (APs) whether connected or not thus ensuring a real time inventory.

h. **IT Training**: MIP management notes that MIP has an annual training budget. The ICT strategy will cater for training that increases MIP productivity.

Chapter 3

a. **Integrated Property Management System**: MIP management notes NAO's recommendation to ensure full use of the system and to keep it updated to reflect the company's business needs and is tackling these matters with its supplier such that discussions are ongoing to amend the contract insofar as details, updating and GDPR matter are concerned.

b. **MIP Website**: MIP management notes that a new website is currently being developed as part of the company rebranding exercise. During the development of the current website, MIP had followed and implemented all direction provided in relation to the Government Website Standards including direction from FITA. The address on the Terms and Conditions page has been updated.

c. **Social Media**: MIP management notes that MIP has been working on an extensive company rebranding which shall also comprise a change in name. Thus, a decision was made not to push social media with the old brand so as not to create confusion once the new brand is launched. Unfortunately, the prevailing context and other circumstances have delayed the launch of the new brand, on which work has been completed for quite a while. This also includes the registration of new pages/channels not just on Facebook, but also on Linkedin, Instagram, and Youtube. Use of these social media channels is set to increase significantly following the launch of the new brand.

Chapter 4

a. **Anti-virus**: MIP management notes that anti-virus programmes are installed on all servers and laptops, that these are console managed and updated. Therefore, the NAO recommendation has already been implemented and is being carried out on a weekly basis.

b. **Patch Management**: MIP management notes that not all users are present at MIP and that there are also hardware limitations since not all laptops and PCs in use can take the updates. It is envisaged that this issue will be sorted out by Q2 2021.

c. **Back-ups**: MIP management notes that back-ups are cloud based and therefore advanced in that "on premises" data is replicated on the cloud and backed up again from the cloud (known as 2+1). Management notes additionally that file versioning is in place and that a random back-up and restore procedure is carried out every first week of the month, which procedure is documented at service provider's end.

d. **Internet Services and Electronic Mail**: MIP management notes NAO's suggestion which will be implemented as part of our ongoing action plan to keep employees well-informed on MIP's policies and procedures.

a. **Risk Assessment Exercise**: MIP management notes that cloud storage automatically ensures back up of data at another premises in the same location. Management also notes that the company has vulnerability management software in place and that an assessment report is issued every Monday.

b. **IT Business Continuity Plan and Disaster Recovery**: MIP management notes that these have been tackled and are in place.

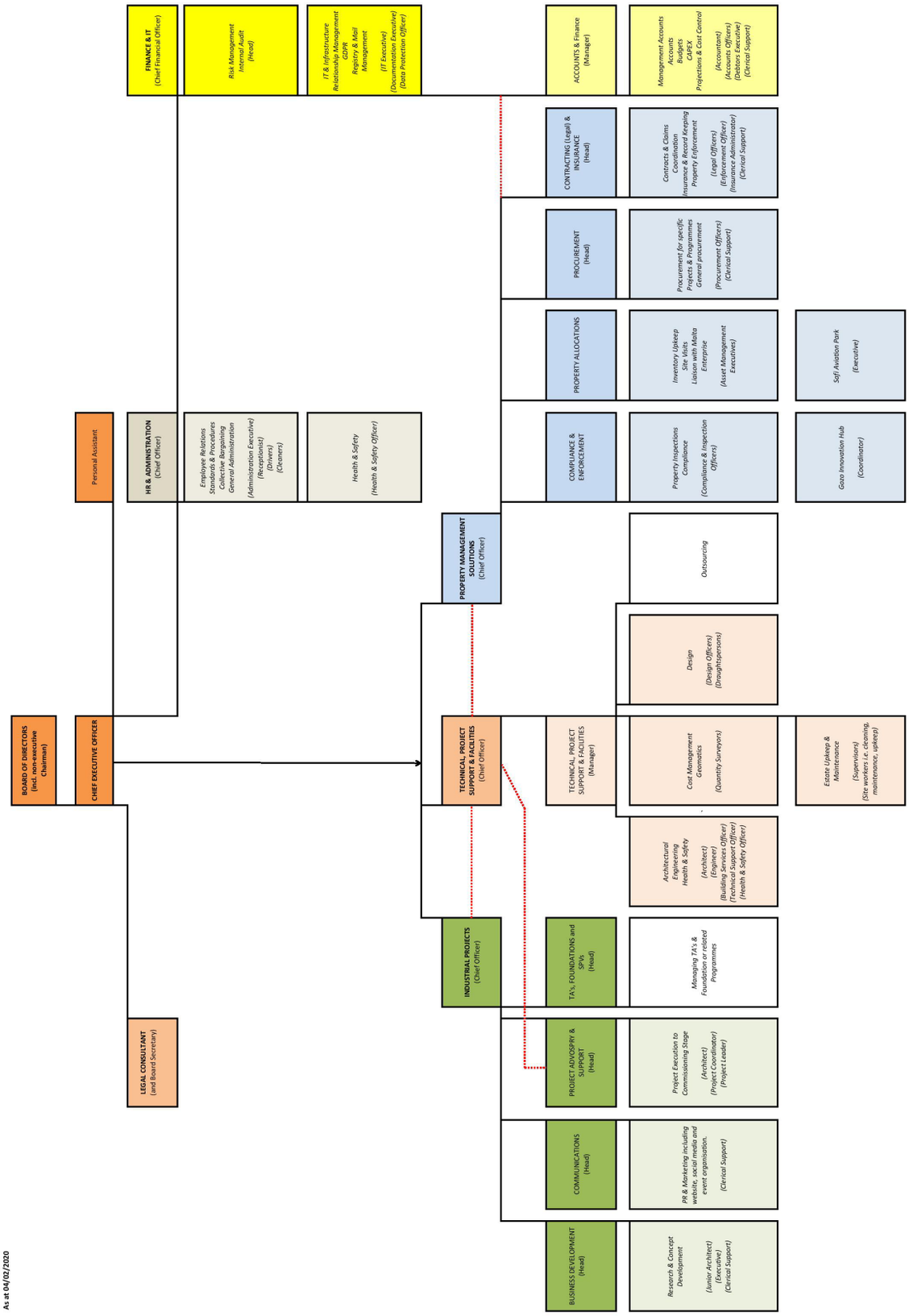
c. **IT Security Awareness Training** – Part of the induction training to new employees includes GDPR which does focus on the importance of information security. We also have a detailed IT User Security Policy as part of our Policies & Procedures Portfolio and which is disseminated to all new recruits. Furthermore MIP has a dedicated Training budget and an ongoing training programme since it is committed to continue offering employees all the necessary training in procurement related topics so they will acquire the knowledge and skills they need to perform their jobs. Information Security Awareness Training will continue being part of this programme.

6.1 Recommendations Implementation Schedule

Components		2021				2022			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Chapter 2 IT Management	IT Unit		X						
	ICT Strategy	X							
	ICT Budget	Already in place							
	Procurement of Hardware	Already in place							
	Procurement of Software	X							
	Hardware Disposal	X							
	IT Asset Management	Already in place							
	IT Training	X							
Chapter 3 IT Applications	Integrated Property Management Solution based on LEMIS	X							
	MIP Website	X							
	Social Media	X							
Chapter 4 IT Operations and Security	Anti-Virus Software	Already in place							
	Patch Management		X						
	Backups, Off-site Storage and Recovery of Data	Already in place							
	Internet Services and Electronic Mail	Already in place							
Chapter 5 IT Risk Management	Business Impact Analysis	Already in place							
	Risk Assessment Exercise	Already in place							
	Business Continuity and Disaster Recovery	Already in place							
	Security Awareness Training	Already in place							

Table 2: Implementation Schedule

Annex A: The MIP Organogram



As at 04/02/2020

Annex B: CoBit Controls

CoBit defines IT activities in a generic process model within four domains[4]. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate as depicted in Figure 6. The domains map to IT's traditional responsibility areas of plan, build, run and monitor.

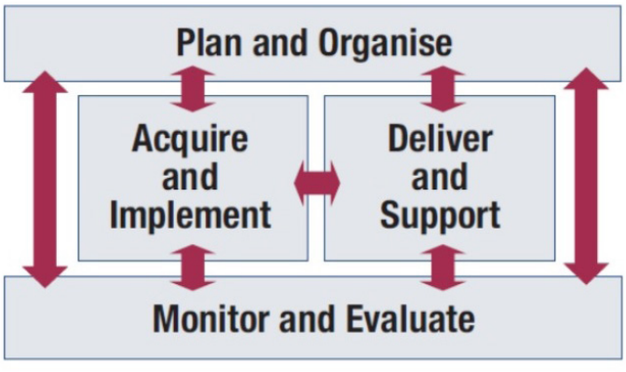


Figure 6: The Four Integrated Domains of CoBit

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 HR 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.

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

Assess and Manage IT Risks

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation, caused by an unplanned event, is identified, 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.

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, and 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 back-up 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.

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.

Annex C: Privacy Policy

The below is an extract from the Government's "Website Content and Presentation Standard" GMICT S 0051-1:2011[5] which may be used as guidance.

Privacy Policy

The Website shall include a Privacy Policy statement stating:

- that any personal information collected shall be stored or processed in accordance with the Data Protection Act[6];
- that any personal information submitted by Website users in a query will only be used to respond to that particular query;
- whether any non-personal information will be collected and if so, which information and the purpose of its usage;
- the information on any cookies used, including why they are being used and what information is being recorded or relayed; and
- the rights of the data subjects as per the Data Protection Act.

[5] https://www.mita.gov.mt/MediaCenter/PDFs/1_GMICT_P_0051_Website_v1.0.pdf
[6] http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12839&l=1

Annex D: Accessibility Statement

The below is an extract from the Government's "Website Content and Presentation Standard" GMICT S 0051-1:2011[7] which may be used as guidance.

Accessibility Statement

The Website shall carry an accessibility statement which declares that the website caters for individuals with disabilities.

Statement shall read as follows: Every effort has been made to ensure that this website is accessible to persons with disability. If you have any difficulty accessing information on this website, please contact us and we will do our best to assist you.

[7] https://www.mita.gov.mt/MediaCenter/PDFs/1_GMICT_P_0051_Website_v1.0.pdf

Annex E: Business Continuity and Disaster Plan[8]

A BCP should:

- be documented and written in simple language and understandable to all.
- be consistent with the Housing Authority's overall mission, strategic goals and objectives.
- provide management with an understanding on the adverse effects on the MIP, resulting from normal systems or service disruption and the total effort required to develop and maintain an effective BCP.
- assess each business process to determine its criticality.
- include a list of essential hardware, software and information assets related to core business processes.
- identify methods to maintain the confidentiality and integrity of data.
- ensure that an appropriate control environment (such as segregation of duties and control access to data and media) are in place.
- ensure that data is regularly backed up on storage media.
- ensure that appropriate backup rotation practice is in place and backups are retrievable.
- ensure that storage media are kept offsite and kept securely in a backup safe.
- identify 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.

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

- include a complete DRP that amongst others lists the access rights granted following a restore.
- validate the RPO and the RTO for various systems and their conformance to MIP's objectives.
- include a plan that details how to restore operations to normality.
- identify the conditions that will activate the contingency plan.
- identify which resources would be available in a contingency stage and the order in which these will be recovered.
- identify the key persons responsible for each function in the plan.
- identify the methods of communication amongst the key persons, support staff and employees to be adopted during recovery of services.
- implement a process for periodic review of the BCP's continuing suitability as well as timely updating of the document, specifically when there are changes in technology and processes, legal or business requirements.
- develop a comprehensive BCP test approach that includes management, operational and technical testing.
- implement a process of change management and appropriate version controls to facilitate maintainability.
- identify mechanisms and decision maker(s) for changing recovery priorities resulting from additional or reduced resources as compared to the original plan.
- document formal training approaches and raise awareness across the MIP on the effect this might have on the entity in the event of a disaster.
- be stored in hard-copy and soft-copy format both on-site and off-site.
- be distributed to members of staff, Head of Sections etc. (any confidential information should only be given to key persons on a need-to-know basis).

A DRP should form part of the BCP and shall dictate every facet of the recovery process including:

- a statement detailing the scope and capability of the DRP, exactly when this plan should be used and what the impact is on the MIP.
- a list of people in the organisation that have the authority to declare a disaster and thereby put the plan into effect.
- ahe sequence of events necessary to prepare the backup site once a disaster has been declared.
- an inventory of the necessary hardware and software required to restore service.
- a schedule listing the personnel that will be staffing the backup site, including, if necessary, a rotation schedule to support ongoing operations without burning out the recovery team members.
- a description of the key roles and responsibilities so that anyone assigned to a particular role in the recovery team understands what is required of him/her.
- a summary of the critical services, their recovery objectives and recovery priorities.
- third party contact details, particularly those that may be required to assist in the recovery of resources or services that are being maintained within the MIP.
- detailed recovery activities and sequence of events, including pre-requisites, dependencies and responsibilities.

2019-2020 (to date) Reports issued by NAO

NAO Annual Report and Financial Statements

May 2020	Annual Report and Financial Statements 2019

NAO Audit Reports

November 2019	Report by the Auditor General on the Workings of Local Government 2018
November 2019	Performance Audit: An analysis of issues concerning the Cooperative Movement in Malta
December 2019	Report by the Auditor General on the Public Accounts 2018
December 2019	An investigation of contracts awarded by the Ministry for Home Affairs and National Security to Infinite Fusion Technologies Ltd
January 2020	Performance Audit: Community Care for Older Persons
February 2020	Performance Audit: Assessing the Public Transport Contract and Transport Malta's visibility on the service
March 2020	Information Technology Audit: ICT across Local Councils
March 2020	The disposal of the site formerly occupied by the Institute of Tourism Studies
April 2020	A review of the ethical framework guiding public employees
April 2020	Addendum Investigation: The Mater Dei Hospital Project
May 2020	Performance Audit: Tackling Child Abuse
June 2020	Follow-up Reports 2020 Volume I
June 2020	Performance Audit: A Follow-Up on the 2016 Analysis on OHSA's Operations - A Case Study on the Contruction Industry
July 2020	An audit of matters relating to the concession awarded to Vitals Global Healthcare by Government Part 1 - A review of the tender process.
October 2020	Follow-up Reports 2020 Volume II
October 2020	Information Technology Audit: Planning Authority