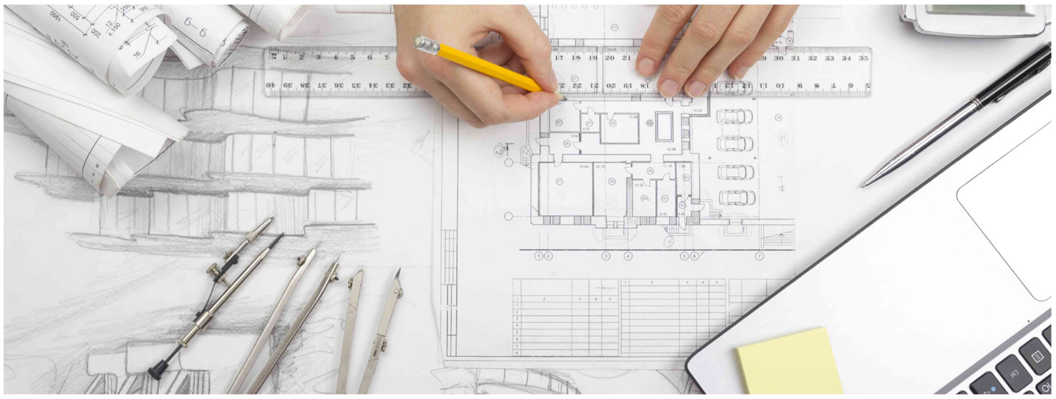
NAO
National Audit Office
MALTA



Information Technology Audit:
Planning Authority

October 2020

Information Technology Audit

Planning Authority

Report by the Auditor General
October 2020

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AD	Active Directory
BCP	Business Continuity Plan
BLC	Building Levy Calculator
CCTV	Closed-Circuit Television
CCU	Close Control Unit
CEO	Chief Executive Officer
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
CPPS	Commuted Parking Payment Scheme
DLT	Distributed Ledger Technology
DNO	Development Notification Order
DoS	Denial-of-Service
DPF	Development Permit Fee
DRP	Disaster Recovery Plan
ERA	Environment and Resources Authority
GIS	Geographical Information Services
ICT	Information and Communication Technology
IT	Information Technology
JRIS	Job Request Information System
LAN	Local Area Network
MEPA	Malta Environment and Planning Authority
MFIN	Ministry for Finance
NAO	National Audit Office
ODZ	Outside Development Zone
PA	Planning Authority
RFQ	Request for Quotation
SLA	Service Level Agreement
UCA	Urban Conservation Area
UIF	Urban Improvement Fund
VLANs	Virtual Local Area Networks

Executive Summary

The scope of this Information Technology (IT) audit was to analyse the overall IT setup of the Planning Authority (PA) focusing mainly on the core IT systems, which were selected for the purpose of this IT audit, namely Artemis, eApplications and the Billing and BLC (Building Levy Calculator) software applications. The scope of this audit was further widened to encompass a review of a selected aspect of PA's document management, namely document retention within the administrative function.

In this context, this audit sought to determine whether the PA has 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 2 of this report focused on the overall IT management of the ICT, Mapping and Digital Services Unit, focusing mainly on the IT infrastructure, maintenance, operations and the initiatives/ projects undertaken by this Unit. The following are the main findings and recommendations included in the above-mentioned Chapter:

a. **ICT Strategy** – Since the PA does not have an official ICT strategy, the NAO recommends that the PA drafts a formal strategic plan for the coming years. This would serve to document the link between the objectives of the current ICT three-year plans and the objectives of the PA's strategic plan.

b. **ICT Budgeting** – The PA requires a policy to ensure that a business case for every major ICT investment is submitted for review during Directors' meetings and that minutes of such meetings are kept as recommended by the NAO.

c. **Disposal of ICT equipment** – The PA stated that the last disposal of assets was carried out in 2015, whereby IT equipment was donated to various charitable institutions. Although the PA could not trace digital documentation related to this disposal of assets, however, the PA stated that the hard disks of the above-mentioned equipment were removed prior to this donation. The NAO recommends that the PA ensures that a record is kept of all the items disposed of in the Hardware Inventory system application, together with a '*Certificate of Destruction*' that would show the number of hard disks that were shredded on that date.

d. **Patch Management** – The NAO recommends that the latest hotfixes and security patches for Windows Server and Microsoft SQL Server instances should ideally first be installed manually on a test environment, and then be deployed on the 'live' servers if no abnormal behaviour is observed. This was recommended as the above-mentioned hotfixes and security patches were being deployed directly on the 'live' servers.

e. **Risk Management** – The PA does not have a BCP and DRP in place, however, the NAO was informed that the PA obtained funds from an EU funded project for consultancy on drafting a BCP and DRP, which will also include a risk assessment exercise. The NAO opines that once this study is concluded both the BCP and DRP are drawn up without further delay.

The following are the main findings and recommendations included in Chapter 3, which covered the core software applications reviewed in this IT audit:

a. **Positive points** – During the execution of this IT audit, the NAO was pleased to note a number of positive findings which are listed below:

- The IT setup at the PA was based on Artemis as the core system, which was fully integrated with the eApplications and the Billing and BLC software applications.

- The core software applications reviewed for the purpose of this IT audit, were hosted on a virtual environment[1] that was installed on a physical server housed at the PA's server room, which was replicated on another physical server at the PA's disaster recovery site.

- The PA ensured that the latest version of the source code of the core software applications reviewed is stored securely. Furthermore, version control was maintained, should rollback be required.

- The PA has integrated both the Artemis and the Billing and BLC software applications with the PA's AD credentials for user access, and thus the same security settings, such as user authentication, are applied to these systems.

- The core systems reviewed for the purpose of this IT audit had a sound audit trail functionality.

- Both the Artemis and eApplications have a to-do list, showing cases (or applications) in hand and the related actions the user is required to take.

b. **Better use of social media platforms** – The NAO opines that the PA is not making best use of social media platforms available to publicise further PA press notices published on the Government Gazette. The NAO recommends that the PA conducts a review of the communication channels used for the publication of such notices.

[1] Some of the main benefits of server virtualization relate to hardware costs, server provisioning and deployment, disaster recovery, energy costs and productivity.

c. **Business process re-engineering** – A procedure for regular business process re-engineering on some of the core IT systems reviewed for the purpose of this IT audit needs to be formalised even though informal reviews have been carried out.

Chapter 4 of this report assessed the extent to which the PA adheres to internal document retention policies and employs formal procedures governing the maintenance of administrative related documentation. The following is a list of the key findings and recommendations included in the above-mentioned Chapter of this IT audit report:

a. **Documentation related to Tenders** – The sampled cases reviewed showed that, in cases where the PA procured goods and services through a tender process, the related documentation was adequate.

b. **Documentation related to Direct Orders** – The PA's document management, including its retention, deviated from generally accepted practices in the following cases of direct orders:

- One case relates to a specific direct order where key documentation was not made available to the requesting source in terms of the Freedom of Information Act. This review could not determine whether the documentation was unavailable because it was either misplaced or not compiled.

- This review noted two other cases where contracts relating to direct orders were not made available to the NAO. Although one would expect that the PA would maintain the full documentation, the NAO sought to retrieve such documentation through other Government entities but to no avail. This implies that the documentation may not have been drawn up at the outset.

c. **Document management processes related to PA's administrative functions** – It is clear that the PA needs to conduct a thorough internal review of its document management processes related to its administrative functions. It is critical that such a review considers the establishment of an organization-wide document retention policy and is complemented with the relative standard operating procedures. The NAO also recommends that the principles adopted for document management related to permit applications is applied to this sector of PA's business processes.

Chapter 1

Introduction

This introductory Chapter provides some background information on the subject under review and looks at some of the organisational changes that the PA underwent in 2016. It also includes the audit's scope and objectives and the methodology used in attaining these objectives, together with a brief summary of each Chapter.

1.1 Setting the context

The PA is the competent Authority under whose responsibility the management of a comprehensive sustainable land use planning falls. This is applicable in respect of both public and private, in accordance with approved policies and plans. The PA seeks to achieve sustainable development throughout the Maltese Islands through the preparation and implementation of development plans and policies, and the processing of planning applications.

The coming into force of Act No. VII of the Development Planning Act 2016 (Cap. 552 of the Laws of Malta[2]) on 4th April 2016, has brought about a new PA following the demerging of the former Malta Environment and Planning Authority (MEPA), in which the organisation reverted to its old name of the PA, whilst all the environmental related issues were passed on to the new Environment and Resources Authority (ERA). Thus, the responsibilities previously assumed by MEPA, are now being handled by the two Authorities, namely PA and ERA, which work independently from each other.

1.2 The Planning Authority

The new PA was set up "*to enhance the quality of life for the benefit of the present and future generations, without compromising the ability of future generations to meet their own needs, through a comprehensive sustainable land use planning system*"[3]. However, to achieve this, the Development Planning Act puts the onus on Government by listing six principles, which although not directly enforceable in a Court of Law, should be '*employed in the interpretation of the other provisions of this Act*'. The six principles mentioned in this Act are:

1. *to preserve, use and develop land and sea for this and future generations, whilst having full regard to environmental, social and economic needs;*

[2] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12451&l=1

[3] Article 3 of the Development Planning Act, 2016.

2. *to ensure that national planning policies are unambiguous, accessible and clear to the general public;*

3. *to deliver regular plans in accordance with the needs and exigencies from time to time;*

4. *to identify regional planning shortcomings and address any problems found in relation thereto;*

5. *to apply scientific and technical knowledge, resources and innovation for the effective promotion of development planning; and*

6. *to consider public values, costs, benefits, risks and uncertainties involved when taking any decisions.*

In addition, the Development Planning Act stipulates that the PA has a number of functions, namely[4]:

a. *to perform and succeed in the functions, which were previously assigned to MEPA under the provisions of the Environment and Development Planning Act*[5] *and are now contained in this Act, and to perform and succeed in the assets, rights, liabilities and obligations of the Malta Environment and Planning Authority established under the provisions of the Environment and Development Planning Act;*

b. *to facilitate and coordinate the permit granting process for projects of common interest; and*

c. *the performance of any other functions as may from time to time be assigned to it by the Minister, including the functions required to give effect to any international obligation entered into by Malta relative to matters regulated by this Act.*

Finally, the Authority '*must execute its duties, functions and responsibilities in accordance with the Government's strategic directions relating to development planning, and as far as possible, refer to European Union (EU) best practices and standards*'.

1.2.1 Organisation structure

The PA has a number of Boards and Committees that assist the organisation to fulfil its functions and responsibilities, in line with its legal obligations. The separation of duties, particularly in decision making, between the Executive Council, which focuses on policy making and administrative functions, and the Planning Board, whose primary role is to decide on development applications, paved the way for more transparency and accountability.

[4] Article 7 of the Development Planning Act, 2016

[5] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=11407&l=1

In addition, the PA operates through five directorates, namely:

1. The Development Management Directorate, which includes the Development Management Division (sub-divided into the Minor Amendments, Sanitary Engineering, Development Notification Order, Billing/Vetting and Regularisation Unit; General Development Unit; the Urban Conservation Area (UCA)/Outside Development Zone (ODZ) Unit; and the Small to Medium-Sized Enterprises (SMEs) and Business Development Unit) and the EU funded, Special Projects and Major Projects Division.

2. The Planning Directorate, which comprises of the Foreign Policy, EU Affairs and Funds Division (sub-divided into two teams, namely the EU and Multi-Lateral Affairs Unit, and the Research and Local Funding Team) and the Strategy and Policy Formulation Division (sub-divided into the Heritage Planning Unit; the Strategic Planning Unit; the Green Blue Development Unit; the Transport Planning Unit; and Planning Control Unit).

3. The ICT, Mapping and Digital Services Directorate is made up of the ICT section (responsible for the PA's network infrastructure, ICT maintenance and programming of all its software applications), Geomatic Services Unit and Operations Unit.

4. The Enforcement and Compliance Directorate, which comprises of the Development Zone, Gozo and Compliance Certification Unit; the Direct-Action Team; the Enforcement Administration Unit; and the ODZ and Sectors Unit.

5. The Corporate Service Directorate, which incorporates the Human Resources Unit; the Business Development Unit; the Finance Unit; and the Debt Collection Office.

At the time of the onsite audit visits, the PA had a staff compliment of 425 employees working on flexible working arrangements, of whom 31 employees work on reduced hours, whilst 70 employees were offered teleworking facilities.

The organogram of each of the above Directorates are included in Annex A.

1.3 Audit scope and objectives

The scope of this IT audit was to analyse the overall IT setup of the PA focusing mainly on the core IT systems, which were selected for the purpose of this IT audit, namely Artemis, eApplications and the Billing and BLC software applications. In this context, this audit sought to determine whether the PA has 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. The scope of this audit was widened further to encompass document management within the PA.

The IT audit was divided into five different stages:

1. The IT audit kicked off with an introductory meeting with the Director of ICT, Mapping and Digital Services Unit, together with the PA's IT manager and the Ministry's Chief Information Officer (CIO), to give an overview of the purpose of this IT audit to the auditee, who, at the same time, provided a brief overview of the PA's current IT setup and ongoing/forthcoming IT-related projects.

2. To understand the complexity of the PA, the NAO scheduled a walkabout with the PA's IT manager and the Ministry's CIO, which visit also served to gather preliminary data, familiarise with the building and see the investments made in ICT, since the demerging took place in 2016, including the modernisation of the PA's existing server room and the implementation of a disaster recovery site, amongst others.

3. Following the above, an in-depth audit questionnaire was prepared and sent to the PA to gather further information on the auditee prior to undertaking on-site audit visits.

4. Subsequently, the NAO managed to carry out a few on-site audit visits and met with key stakeholders to obtain their views on the use of the core IT systems being audited for the purpose of this audit, namely Artemis and eApplications. Unfortunately, in view of the circumstances resulting from the COVID-19 pandemic, the NAO had to cancel all the remaining on-site audit visits and limit the number of meetings held directly with the rest of the key stakeholders within the PA. Instead, the NAO held a few online meetings and rely on emails to address any issues or to clarify pending enquiries based upon the information originally submitted in the audit questionnaire and the meetings carried out with key stakeholders.

5. Finally, the NAO delved into document retention related to the administrative function of the PA due to certain concerns that were reported to the NAO by third parties as well as issues raised by the Information and Data Protection Commissioner regarding the PA's document retention procedures.

In this context, the main objectives of this audit report were to:

- Document all the information gathered from the audit questionnaire and the interviews held with key stakeholders and officials within the PA.

- Summarise the documentation received and highlight areas of concern.

- List all the findings and identify any potential risks.

- Finally, draft a set of recommendations to mitigate such risks.

1.4 Audit methodology

To reach the above objectives, the NAO reviewed the annual reports that the PA had published and uploaded on its website, and the current legislation that regulates the PA's functions and responsibilities.

In addition, and as already mentioned above, the NAO drafted an in-depth audit questionnaire, which was sent to the auditee in the beginning of 2020. The undertaking of this IT audit was then based upon the feedback received from the audit questionnaire, policies and procedures, reviews of contracts entered with third parties between 2013 and 2019 and on-site audit visits and meetings held with key stakeholders.

Reference was also made to the Control Objectives for Information and related Technology (COBIT)[6] set of best practices, some of which were considered during this IT audit. COBIT provides good practises across a domain and process framework in a manageable and logical structure, to help optimise IT-enabled investments, and ensure that IT is successful in delivering against business requirements.

1.5 Structure of the report

Following this introductory Chapter, the audit report includes four further Chapters, each documenting all the data that was collected, highlighting the findings and recommendations:

- Chapter two deals with the overall IT management of the ICT, Mapping and Digital Services Unit, analysing the way in which ICT resources are being managed, focusing mainly on the IT infrastructure, maintenance, operations and the initiatives/projects undertaken by this Unit, and how the Unit maintains the confidentiality, integrity and availability of data.

- Chapter three reviews the core software applications that were selected for the purpose of this IT audit.

- Chapter four deals with document management, specifically retention of documents of 15 randomly selected contracts out of the 81 that the PA entered with third parties during 2013 to 2019.

- Chapter five lists all the management comments submitted by the PA.

1.6 Acknowledgements

The NAO would like to express its appreciation to all the key stakeholders within the PA who were involved in this audit, in particular the Director for Corporate Services, the Director of ICT, Mapping and Digital Services Unit, together with the PA's IT manager, the Ministry's CIO and officials from within the PA, for their time and assistance.

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

Chapter 2

ICT, Mapping and Digital Services Unit

2.1 Background information

The establishment of a new Directorate for ICT, Mapping and Digital Services came into force in 2017, in preparation for the implementation of the SIntegraM application, a €7 million project, part-financed by the European Regional and Development Fund, to replace the existing base map, develop the first national spatial data infrastructure and update Malta's maps. The emphasis of this intensive investment was on providing an optimum network infrastructure, new hardware equipment, and information security controls, to ensure that the Authority continues to provide better services to its clients.

At the time of this IT audit, the ICT, Mapping and Digital Services Unit was made up of around 124 officials and is subdivided into three main sections, namely ICT, Geomatic and Information Services, and Operations.

The ICT section is responsible for the overall upkeep of the PA's network and server infrastructure, the maintenance and support of all the IT equipment, information security, and risk management. The ICT section is also responsible for the development and support of all the PA's software applications, including Artemis, eApplications portal, the internal and external geoportals, the plotting geoportal, the PA's mobile application, and the internal Human Resources systems, amongst others.

The Geomatic and Information Services section is subdivided into four different units, namely:

1. Mapping Unit – focusing mainly on the upkeep of the base maps of the Maltese islands and to provide mapping related services to the PA's front desk.

2. Land Surveying Unit – responsible for marking street and building demarcation lines, and to conduct topographic survey plans.

3. Alignment Interpretation Team – works closely with the Land Surveying Unit, to interpret the alignment and survey plans for the establishment of street and building demarcation.

4. Information Resources Unit – upholds its significant role of spatial data creation and analysis across all Directorates through thematic spatial data modelling and reporting, and the management of EU related projects.

Finally, the Operations section is subdivided into six different teams, namely:

1. Operations Team – maintains the PA's statistics, which are either used for performance measures, or are related to a specific parliamentary question. It also provides assistance in bridging the gap between other Directorates and software developers within the ICT section, and assists in all process re-engineering, which may include process analysis, legal notices and the drafting of circulars.

2. Mailroom Team – responsible for printing of all the permit plans, uploading of physical correspondence onto Artemis, sending of fresh plan notifications, and for the distribution of physical documentation.

3. Documents and Records Retention Team – retains and distributes old records prior to 2006, and to overview the digital scanning process.

4. Initial Vetting Team – receives and checks all incoming planning applications for completeness of documentation.

5. Plotting Team – Geospatially plot planning applications, which are processed either as: an outline development; full development or a summary development procedure application; development notification order (DNO)[7] applications used for minor works; regularisation process applications for non-sanctionable development with the development boundaries; and dangerous structure applications to remove an existing structure, which is considered to be unsafe for use by all the PA officers and for use by the general public through the PA's Geoportal.

6. Customer Care Team – provides customer care services at the front desk, by email or phone, to ensure that there is continuous communication with applicants, for instance: informing them of important deadlines relating to their applications; handling complaints received relating to alleged development illegalities; and providing feedback to general queries received on a particular application.

During the course of the IT audit, the NAO looked into the operational aspect of the ICT section across the PA, and how technology has changed the PA's business processes becoming more integrated and streamlined.

[7] A DNO is the simplest form of application that can be submitted to the PA. Within the DNO, there are 22 classes and the types of developments permitted through this procedure, listed in the Classes, are usually those which do have a negative impact on the respective neighbourhood. Some forms of development listed in specific Classes can be carried out without any form of notification to the Authority – Subsidiary Legislation 552.08 – Development Notification Order (http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=11557&l=1)

2.2 ICT Strategy

The NAO was informed that whilst the PA has no formal ICT strategy document, over the past years, the PA has introduced an efficient and cost-effective ICT strategy, whereby the processing system of each planning application is nowadays totally paperless, and all the applications are thus being submitted and managed online. This was achieved through the investments made in the PA's network infrastructure, servers, IT equipment, the introduction of new IT systems (ex. Artemis, SIntegraM and eApplications), virtual applications, a new telephony system, and the digitization of all its processes.

In addition, the measures taken by the PA, in adopting this digitization process, give its employees the flexibility of being able to telework, thus offering better family-friendly measures. Such flexibility was not only beneficial to the employees but ensured that the PA could continue being productive with fewer employees opting for reduced hours, providing adequate human resources, to make sure that it could continue offering a timely service to its clients.

Meanwhile, the NAO was informed that all ICT projects are listed in a three-year plan and monitored on a quarterly basis in project plans, which are updated on a monthly basis by the Director of ICT, Mapping and Digital Services Unit together with Senior Management.

Furthermore, the NAO was also informed that the ICT plans are based on the outcomes of meetings at Directors' level, attended by the Director of ICT, Mapping and Digital Services Unit, and chaired by the Executive Chairman, however, minutes of these meetings are not taken. These meetings cover topics such as planned changes related to workforce levels, working practices, legislation and policies, which may all impact ICT operations in one way or another.

2.3 ICT budgeting and investments made across the Planning Authority

At the time of the IT audit, the NAO was informed that the annual budgeting exercise involves an assessment of the organisation's ICT requirements, in terms of both the recurrent and capital expenditure for the forthcoming three years. Due consideration was also given to anticipated increases in the workforce, changes in internal processes and working arrangements, the long-term ICT strategy and hardware replacement policies.

The NAO was also informed that when the PA reviews proposals for ICT investments, it does so in an informal manner, and the review does not require the submission of a formal written business case for the investment proposal showing the proposed investment's scope, benefits, costs, resources required and timeframes.

As highlighted earlier above, following the preparatory work undertaken in 2015, the PA submitted an application on behalf of the Government of Malta for the funding of the SIntegraM project in 2016, and eventually managed to secure €7 million to carry out this project, mostly funded by the EU. Through this project, the Government of Malta aims to develop and implement a national spatial data infrastructure and enhance the capacity of geo-spatial/GIS technology expertise for Malta. The SIntegraM project constitutes the creation of a strategic approach to spatial data, creation of critical base datasets, as well as enabling a legislative and mentality shift in terms of exchange and access to data. The project will ensure that the underlying aerial, terrestrial and bathymetric infrastructure and knowledge gain is made available to all Government entities in order to assist these entities in delivering the relevant analytical framework as required under national, EU and other international obligations. Ultimately, this project will enhance spatial data and collaboration within Government.

Following a decision taken by senior management to adopt a paperless environment, in 2016 the PA commenced a digitization project whereby past records and documents started being scanned, such as accounting and human resources records. The aim of this project was to reduce the management of paper and facilitate the archiving and retrieval of past documents. Over the span of two years, the PA invested over €1 million in ICT infrastructure, and through this investment, it continued to digitize more of its processes, including amongst others, the Planning Control, Reconsideration and Grant Scheme, and the Building Alignment applications. Nowadays, the processing of each planning application is totally paperless.

Apart from the above, in 2018, the PA also invested in increased bandwidth to improve the network connectivity for external users, thus ensuring that the PA's services are always readily available. The increase in bandwidth paved the way for the PA to adopt a number of family-friendly measures for its employees, including the implementation of virtual applications, and the installation of a soft phone telephony system. Such a system gives employees the flexibility to telework and communicate through video conferencing with other employees and external users, such as architects, and to discuss any salient issues related to any planning application.

2.4 The operational aspect of the ICT unit within the ICT, Mapping and Digital Services Unit across the Planning Authority

As highlighted in the beginning of this Chapter, the NAO looked into the operational aspect of the ICT section, within the ICT, Mapping and Digital Services Unit, focusing mainly on how the ICT section is managing the PA's ICT services and supporting the overall network and server infrastructure.

2.4.1 Management of IT hardware equipment

The NAO reviewed the process involved in the procurement, maintenance and disposal of IT hardware equipment and the software development lifecycle in terms of planning, development, testing, implementation and maintenance of software applications, most of which are developed in-house within the ICT, Mapping and Digital Services Unit.

Procurement of ICT equipment or service

In terms of the procurement of ICT equipment or service, the ICT section adheres to the Government procurement procedures[8], with the use of the Electronic Public Procurement System (ePPS) for all calls for tenders. The ICT section also receive guidance from the PA's Procurement Office when the need arises. In this context, the ICT section is responsible for the technical specifications and where necessary for the evaluation of supplier submissions.

In addition, the NAO observed that the PA also adheres to an internal procurement procedure, which was initially drafted in May 2017, and was last updated in June 2019. This procedure describes the methods applied and the personnel responsible for purchasing any product or service. Once a request for the procurement of a product or a service is approved by the Director of ICT, Mapping and Digital Services Unit, the request is recorded on the Job Request Information System (JRIS)[9] by the PA's ICT Helpdesk Team, who in turn forwards the request to the team responsible for the purchase.

Once a request is processed, the officer managing the procurement process will liaise with the internal Purchasing section to identify the correct procedure and compile the latest procurement forms described by law. Then the officer in charge may either makes a request for quotation (RFQ) to a selected number of suppliers, publish an RFQ in the Government Gazette or makes a call for open tenders, which is published on the Department of Contracts portal (ePPS application). However, there may be instances whereby the PA has to opt for an ad-hoc procurement, which requires a direct purchase due to the urgency attached to procurement. This method of procurement is only used where a purchase is pre-approved and requested by the PA's Executive Chairman and/or the requested items are required urgently.

The quotations or open tenders submitted, are then evaluated to confirm that the bids conform to the specifications defined in the initial stages and then determine the award of the bid, based upon:

- the most economically advantageous offer;
- the lowest price offered is compliant with the specifications set; or
- a negotiated procedure.

[8] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=9532&l=1

[9] The JRIS was created internally to handle all the requests raised by all PA officials.

Upon approval, a purchasing order is issued for the procurement of the product or service, from the selected product or service provider, and on receipt of the product or service, the officer in charge will verify whether:

- the product or service conforms with the specifications stipulated in the tender or quotation as awarded;
- the product or service is complete; or
- the product is damaged or defective.

Finally, the requested specifications are re-evaluated with every RFQ, and a tender is issued based upon the submissions from suppliers, product or service offered, and any appeals or clarifications received during the whole process. This re-evaluation exercise would then establish whether the specifications used for the tenders need to be improved for future specifications in similar products or services required.

Maintenance and support

The ICT section offers first-line and second-line technical support to all the end-users within the PA, which includes the servicing and repairs of IT hardware equipment, such as PCs, laptops, tablets, printers, scanners, plotters, etc.

In the event that technical assistance is required, the NAO was informed that all PA officials are requested to contact the ICT Helpdesk Team, which is manned on a roster basis by technical officers from within the ICT section, and all requests are recorded in JRIS. The latter is used to record, set deadlines, as well as monitor the progress of all user requests, log approvals of the user's immediate supervisor where applicable, and add any additional information needed to service the user's request. In addition, the system will automatically record any modifications done to the job request, record any communication with the customer (the user raising the request), log any comments, feedback or complaints received by the customer in the *Request log history*.

In this regard, the NAO noted that in 2017, the ICT section had drafted a procedure on how requests are managed in JRIS. This procedure was then updated in 2019, to include an Annex with a user requirements list depicting to whom such requests are assigned within the ICT section to service the call. For instance, in the event that a customer experiences hardware problems with his/her laptop, the Network and PC Support Team within the ICT section would first check with the Hardware Inventory system application when the item was procured and if the laptop is still under warranty, they will contact the local supplier to service it accordingly. On the other hand, if the laptop is no longer under warranty, the Network and PC Support Team would carry out the necessary repairs. If it results that some parts need to be replaced to repair the laptop, then the supplier is contacted to provide a quotation and then a decision is taken internally whether it is feasible to repair the laptop or else place for disposal.

In terms of hardware and software inventory, the ICT section keeps track of all the IT hardware equipment in a Hardware Inventory system application, which was developed internally. In addition, the ICT section maintains a separate detailed inventory of all the software applications procured and installed on PA workstations. In this regard, the NAO noted that in 2017, the ICT section had drafted an internal procedure to keep track of software licences and ensure that any renewals required to retain use of software licences, Secure Sockets Layers (SSL) certificates[10] and Domain names are carried out in a timely manner. Similarly, in 2019, the ICT section had also drafted an internal procedure for the management of ICT hardware assets, that is, the process that is followed to record, manage and maintain all the ICT equipment within the PA, and keep track of any ICT equipment that is loaned to PA officials.

Disposal of IT hardware equipment

In terms of the disposal of IT hardware equipment, the NAO looked into the procedure adopted by the ICT section to dispose of the IT equipment that is either obsolete or beyond economical repair. In this regard, the NAO noted that the internal procedure mentioned above, relating to the management of ICT hardware assets, also documents the procedure adopted for assets, which are either obsolete and need to be replaced, or are not feasible to repair. Whatever the outcome, the asset is marked as '*Disposed*' in the Hardware Inventory system application and placed in store with other devices for disposal. The NAO was informed that all the assets that are to be disposed of are stored until a large enough quantity of assets are put together. When this is the case, the PA engages a third-party subcontractor to collect and dispose of all the IT hardware equipment. The NAO noted that the last disposal of assets was carried out in 2015, whereby IT equipment was donated to various charitable institutions. In this regard, the PA stated that the hard disks of the above-mentioned equipment were removed prior to the donation.

2.4.2 Software Development Lifecycle

The software development lifecycle is a systematic process for building software applications to ensure the quality and correctness of the software built.

The NAO noted that almost all the software applications in use across the PA were developed in-house by a group of software developers who work with the Application Development and Support Team within the ICT section. Rather than using the traditional sequential waterfall model, the Application Development and Support Team has recently adopted an agile software development lifecycle approach. Such an approach involves an iterative consultation process with the end user throughout the software design and programming process. In other words, the agile approach embraces the constant changes that prevail in software development processes, whereby software developers can develop working software in small quick steps and releases updates more frequently. Every new release serves as a base for the next one and therefore the software developer must complete a phase before moving to the next.

[10] SSL certificates, also referred as a Digital certificate, creates a secure link between a website and a visitor's browser. By ensuring that all data passed between the two remains private and secure, SSL encryption prevents hackers from stealing private data, such as credit card numbers, names and addresses.

The NAO was informed that in 2017, the PA had drafted an internal policy on the design and development of software applications. This procedure is applicable to all the software packages, which were designed and/or managed by the Application Development and Support Team. The NAO noted that the team adopts two different procedures in software development, namely:

- Process A: high level project evaluation – such a project would involve significant software development, or significant upgrades or maintenance to existing software.

- Process B: modular design and development – this process involves the design and development of a particular software module.

An important aspect in the software development lifecycle is system testing. Ideally, testing is carried out by someone other than the software developer, whose assessment of the software is objective and impartial. In this context, the NAO noted that the Application Development and Support Team gives importance on system testing by drafting a test plan, which includes items to be tested, testing method, pass/fail testing criteria, the order in which tests are carried out and the expected outcome of each test. Unexpected results encountered are reported as bugs and recorded in a fault reporting package for action to be taken by the respective software developers. Finally, before the system is signed off and accepted by the system owner, the tested solution is moved to the user environment for the final user acceptance testing and review.

2.4.3 Network and Data Centre Infrastructure

A network infrastructure is a branch of IT services that provides a network on which different devices can connect, communicate and operate together. Hardware, software, IT services and facilities all fit under the network infrastructure umbrella, whereby users can communicate efficiently and easily via various means such as email, instant messaging, videoconferencing, telephony, etc. It also provides access to information through the sharing of files, data and other types of information, giving authorised users the ability to access information stored on other computers or servers on the network, or to access and use resources provided by devices on the network, such as printing a document on a shared network printer.

As mentioned earlier above, the PA invested heavily to have a robust network infrastructure. The latter is connected to a local third-party service provider and has multiple paths and links available to any given destination within the main office block area. This kind of setup is vital in terms of load distribution, as it determines the flow of traffic and the efficient use of resources. In addition, the PA network infrastructure is also equipped with high-performance security appliances that determine the incoming and outgoing network traffic flow.

In terms of the Local Area Network (LAN) infrastructure, the PA network is logically segmented into a number of Virtual LANs (VLANs). The latter logically separates and isolates certain traffic from other traffic on the network, whether it is data, voice or other. The segregation of the LAN into VLANs offer a number of benefits in terms of security, cost reduction, better performance, improved IT staff efficiency and simpler project and application management amongst others. The PA also has a number of Wi-Fi hotspots, which are segregated from the PA's corporate network and are even connected to a different local third-party service provider.

The Network and PC Support Team, within the ICT section, maintains and supports the PA's network and server infrastructure. This includes the daily monitoring of all the network hardware, including routers and switches, monitoring and upkeep of both the physical and virtual servers, technical support on both the WAN and LAN infrastructure, and the overall maintenance of the physical and environmental access controls within the main server room and disaster recovery site.

The NAO observed that the PA has recently refurbished its server room where all the servers, storage devices and network equipment are installed. At the time of the IT audit, works were also underway to replicate some of the server equipment at the disaster recovery site, so that in the event of a server malfunction or a disaster at the server room, the Networks and PC Support Team could manually fail-over on to the servers hosted at the disaster recover site.

To ensure that all the data and IT equipment are safeguarded across the PA, the NAO also reviewed the physical access and environmental controls in place, mainly at the PA's server room and disaster recovery site. In this regard, the NAO observed that both the server room and disaster recovery site are restricted by card access controls and only a few authorised personnel from within the Networks and PC Support Team can gain access to these rooms. In the event that maintenance on servers or the air-conditioning system is required for instance, the third-party supplier is always accompanied by someone from the Networks and PC Support Team.

Meanwhile, both the server room and disaster recovery site are equipped with Closed-Circuit Television (CCTV) cameras and thus, whoever gains access to both rooms is captured from the CCTV recordings. In addition, a list of who accessed the rooms, including the date and time of access, can also be retrieved from the access card system. The NAO noted that CCTV cameras are not only installed inside the server room and disaster recovery sites, but also inside the main office building, at strategic entry points, carparks and the external perimeter of the PA offices in Malta and Gozo.

All the CCTV recordings captured by the system are kept for 15 days, after which time, the images are automatically overwritten. If a specific footage is required for an investigation, the relevant extract will be retained until the investigation is concluded. The NAO was informed that access to and disclosure of images is restricted and carefully controlled, not only to ensure that the privacy rights of the individual are preserved, but also to ensure that the chain of evidence remains intact should the images be required for investigative purposes. It is to be noted that an audit trail is kept showing details of who gained access to these logs, date and time and reason for access.

Finally, in terms of environmental controls, the NAO observed that both the server room and disaster recovery site are equipped with smoke detectors and an Argonite fire suppression system[11], whilst fire extinguishers are located outside the server rooms. Having said that, the NAO was informed that smoke detectors and a few heat detectors are also installed throughout the PA's main office building, whilst a number of fire extinguishers are located in strategic locations within the building. These fire extinguishers are inspected and serviced annually by a local third-party supplier.

To ensure that the network and server equipment operate at the right temperature and humidity levels, the NAO noted that the server room has three sets of Close Control Units (CCU), which are configured to rotate between each other to maintain the temperature and humidity levels together to a precise set level. The CCUs are equipped with an auto dialler and set up to notify ICT officers from within the Networks and PC Support Team with an SMS, in the event of technical faults or if the set temperature threshold has been exceeded. Similarly, the disaster recovery site is equipped with three split air conditioning units and the temperature is monitored through a specific software application, which is configured to send an email to ICT officers, from within the Networks and PC Support Team, if the maximum temperature threshold has been reached.

Finally, in the event of a power failure, both the server room and disaster recovery site are connected to two separate Uninterrupted Power Supplies (UPS) to safeguard all the servers, storage devices and networking equipment, from any power surges or unexpected shutdown.

2.5 Information Security Management

With the development in ICT and increasing accessibility to the Internet, organisations are nowadays becoming more vulnerable to various types of threats, which may come from different sources like employees' activities (internal) or hacker (external) attacks. Thus, if the ICT infrastructure is not secure, this presents a significant vulnerability to various attacks such as Denial-of-Service (DoS), malware, spam and unauthorised access. In view of this, the NAO reviewed the security measures implemented by the PA to ensure that it is sensibly protecting the confidentiality, availability, and integrity of its IT systems and data from any threats and vulnerabilities.

2.5.1 Identity and Access Management

Identity and access management is the process of establishing and verifying one's identity to ensure that authorised users can only access to what they require.

[11] Argonite fire suppression system uses an inert gas that offers effective fire protection with zero environmental impact, by physically removing oxygen from the atmosphere.

User Account management

In order to verify the identity of a person, every user is provided with a login (which is uniquely identifiable) and a password. In this context, the NAO noted that all the requests for the creation, modification, disabling and deletion of user accounts, in terms of Internet, email and Domain accounts, are handled internally by the Networks and PC Support Team, once an incident is raised by the ICT Helpdesk Team on JRIS. All user accounts are created on the PA's Microsoft Windows Active Directory[12] (AD) server and then granted specific access privileges to certain directories/ folders and software applications residing on a server. The NAO observed that user accounts are well organised into logical groups and subgroups, providing access controls at each level.

Password Management

Passwords on the other hand are a primary means to control access to systems and should therefore be appropriately selected, used and managed. Passwords provide the first line of defence against improper access to data, which may compromise sensitive information.

In this context, the NAO noted that every password must be set with a minimum number of characters, which must meet password complexity requirements, whilst the use of previous passwords is not allowed. In addition, the user must change the password upon first logon and every password is set to expiry over a period of days. In the event that the user has forgotten his/her password, the user must request a password change, whereby a random password is generated and sent to the user via SMS to his/her personal phone. If the user does not have access to their phone, they have to physically go to the Networks and PC Support Team's office to collect their newly generated password. Every new password generated must be changed again upon first logon.

In the meantime, the NAO noted that generic administrative passwords of servers and software applications are kept in sealed envelopes and securely stored in a safe. These passwords can only be accessed by the ICT manager and the responsible officer for backups, whenever an emergency need arises, in the event of hardware system or software application failure. In the case of Microsoft Office 365 administrative accounts, these have been set with a two-factor authentication through the use of a password and a randomly generated token, which is sent to the user's personal mobile phone.

[12] The AD is a directory service that centralises the management of users, computers and other objects withing a network. It's primary function is to authenticate and authorise users and computers in a windows domain.

Audit Trails

In line with identity and access management, auditing is another important process, as it provides basic information to backtrack through the entire trail of events usually to the original creation of the record. This may include user activities, access to data, login attempts, administrator activities, or automated system activities. In other words, auditing provides the necessary trail to explain who, what, when, where and how resources are accessed across the network.

Login and security audit trails are retrieved by an audit server, which was installed for the sole purpose of polling all the audit logs from the AD servers and flat file data servers. Such logs are backed up and not deleted after a period number of days. In fact, the NAO was informed that the PA can retrieve audit logs dating back to 2015. In addition, all workstations keep a record in the event log, which is only accessible if a user has logged on to a workstation with administrative privileges. However, such logs are stored locally on the workstation and are not being backed up.

The NAO also observed that the software applications there were selected for the purpose of this IT audit, (Chapter three refers), have an audit trail functionality that records amongst others the successful or failed logon attempts according to date and time. One of the software applications in question, Artemis, also has a *Minutes* tab whereby every document that is uploaded in the system, is automatically 'minuted' in this tab, recording the date and time and who uploaded the document.

2.5.2 The measures being taken to mitigate cyberattacks and to protect the Authority's data

The NAO reviewed some of the measures the ICT section is taking to mitigate against cyberattacks and to protect the Authority's data.

Limiting employee access to the organisation's data and information

Limiting access to the organisation's data reduces the chances of human error, which is considered as the number one information security threat. Various studies on this matter show that employee mistakes, negligence or malice are frequently the cause of data loss. In this scenario, the best approach is to practice the principle of least privileges, whereby employees should only have access to the systems and specific folders/documents they need to do their jobs, and then add user privileges if the need arises. When access to sensitive data is no longer required, all corresponding privileges should be immediately revoked. Thus, in the event that an employee leaves the organisation or moves to a different Directorate or section within the organisation, protective action should be taken immediately, which may include deleting or disabling of user accounts from all systems. Similarly, all user passes/ID badges or entry keys, should be collected when an employee leaves the organisation, whilst access to folders previously used by the individual in his/her last post within the organisation should be revoked.

In this context, the PA's HR Unit informs the ICT Helpdesk Support Team when a user's employment has been terminated and an incident request is raised on JRIS to lock the user's login account on the PA's AD server. In doing so, the user's account is also locked on all the software applications that are integrated with the PA's AD server to gain access to the respective system. A similar approach is adopted for employees on prolonged leave, career break or maternity leave. In this scenario, the HR Unit will determine when to inform the ICT Helpdesk Support Team, if a user login account is to be disabled or temporarily disabled, since there might be instances whereby the HR Unit has made arrangements for the individual to telework during the period of absence.

Malware protection

To safeguard against cybersecurity risk, such as the spread of malware[13], an antivirus protection software must be installed and updated regularly. Most antivirus protection software suites are updated almost daily with the latest fixes to security exploits, ensuring systems are as safe as possible against virus outbreaks. If a virus signature is detected, the antivirus protection software will simply intercept and quarantine the virus, preventing it from spreading onto other systems.

The NAO noted that an antivirus protection software is installed on all workstations and servers, which is updated continuously through a master server (that acts as a relay with the vendor's cloud services). The master server downloads continuous updates by the hour and then pushes them on to the workstations connected to the PA's network domain. Moreover, the antivirus protection software was configured to run quick scans daily, once a workstation is switched on, whilst a full scan is scheduled to run randomly once a week.

Patch management

The NAO was informed that the PA's workstations are configured to automatically download and install product updates over the network, to ensure that all the software applications and operating systems are patched with the latest security and operational patches from the vendors, and resolve the latest known exploits and vulnerabilities. On the other hand, Windows servers, as well as Microsoft SQL server instances, adopt a slightly different approach whereby hotfixes, patch releases and service packs are downloaded and installed manually on the 'live' environment, and then the required server reboot is scheduled accordingly.

Security awareness training

Continuous employee education is of fundamental importance in protecting data and securing information systems. It is thus highly recommended that security awareness should be part of an ongoing process that seeks to ensure that all the users are familiar with the information security

[13] Malware is shorthand for malicious software, which is a software that is developed by cyber attackers with the intention of gaining access or causing damage to a computer or network, often while the victim is unaware that there's been a compromise. Malware spans everything from the simplest computer worms and trojans to the most complex computer viruses.

policies and best practices that govern the use of IT assets. This can be disseminated either using emails, through the publication of leaflets and handbooks, or communicated verbally, to ensure that the information is communicated to the users in a timely manner.

Security awareness should typically include information about the latest security trends, such as ransomware, phishing, spyware, rootkits, DoS attacks and viruses. Employees should learn, for instance, how to spot fake URLs and attachments with bogus macro-codes embedded within, as these can be used to harvest data[14] from a compromised system.

In this context, the NAO was informed that in the beginning of 2020, all PA employees attended cyber awareness information sessions. From the feedback received, these sessions were very fruitful, as practical examples were given during these sessions, making them aware of the potential risks that each individual may be exposed to. Apart from these sessions, email shots are regularly disseminated, especially when a malicious email is encountered, and users are advised to delete such emails should they receive them in their mailbox.

Security monitoring

Another important process to mitigate cybersecurity risks is to monitor the network traffic for any suspicious activity. This can be achieved through several intelligent platforms available that will monitor the organisation's infrastructure and send an alert on any anomalous activity, as well as to generate trend analysis reports, monitor network traffic, report on system performance, and track/monitor system and user behaviour.

In this context, the NAO was informed that the PA has invested in server and network monitoring tools, including a Network Performance Monitor (NPM) software application that can quickly detect, diagnose and resolve network performance problems and outages, and a similar network monitoring tool that can monitor and classify system conditions like bandwidth usage or uptime, collect statistics from miscellaneous hosts such as switches, routers and other devices, and also monitor all types of servers in real time in terms of availability, accessibility, capacity and overall reliability.

Intelligent monitoring tools and equipment, such as firewalls and internet gateways, were implemented to detect and block executable downloads, block access to known malicious domains and manage users' access to the Internet. Furthermore, the PA has also implemented a Security Information and Event Management (SIEM) tool, which scans server logs and detect any unusual patterns of users or server activity.

[14] Data harvesting is a process where a small script, also known as a malicious bot, is used to automatically extract large amount of data from websites and use it for other purposes.

Internet and email content filtering

Nowadays, the Internet and email services are considered as mission critical services in any organisation to communicate internally as well as externally to customers, services providers, Ministries and other Government entities. The NAO was informed that whilst the email services are provided and managed internally by the ICT section, the Internet service is provided by a local third-party service provider, but at the same time it is being managed by the ICT section.

In this context, the NAO noted that all the PA employees adhere to the email and Internet usage policies, which were drafted by the ICT section in 2013. The '*Email Usage Policy*' stipulates that the email service is provided for official business use only and thus all the email messages created and transmitted on the PA's workstations are the property of the Authority. As a result, following approval from senior management, the PA reserves the right to investigate any and/or all usage of emails, and all the files, information, software and other content created, sent, received, downloaded, uploaded, accessed, or stored in connection with user usage.

The ICT section has implemented an email filtering system to filter all inbound and outbound email traffic and automatically detect certain types of content that may be potentially harmful. In terms of inbound email filtering, the system scans all the messages addressed to users and classifies the messages into different categories, which include but are not limited to spam, adult, bulk, virus, impostor and others. Email messages that may contain scripts and executable code, compressed files (ex. *.zip* and *.rar*), foul language, sound files and videos as an attachment, are rejected automatically by the system. However, in the event that legitimate emails are rejected and classified as spam (such as messages coming from a legitimate email mailing list but happens to contain text that makes it appear to look like spam), the user is requested to contact the ICT Helpdesk Team to rectify the issue. In addition, the ICT section makes use of sandboxing, which opens and inspects attachments in emails, which may contain malicious macros or executables, in an effort to mitigate system failures or software vulnerabilities from spreading.

Similarly, every user is responsible and held accountable on the use of the Internet. Thus, the PA reserves the right to monitor the volume of Internet and network traffic, together with Internet sites visited. In this context, the NAO noted that the PA has set up an Internet usage filtering system that automatically logs any use from all computers and devices connected to the PA's corporate network. All the inbound and outbound Internet traffic is monitored, whereby the system will record the source IP address, the date and time, the protocol, and the destination site or server. The system can also record the user login of the individual and blocks access to Internet websites and protocols that are deemed unsafe or inappropriate for the Authority's corporate environment. Sandboxing is also implemented to prevent malicious code being downloaded by the end users.

To achieve this, the PA has adopted a checkpoint three-tier architecture, classified as bronze, silver and gold, whereby different users are grouped into one of these tiers. Each tier has a number of allowed/blocked categories for browsing. Having said that, there may be instances whereby some exceptions are made, such as to grant additional Internet access to particular websites to specific users due to their work exigencies, however these require approval by management from time-to-time.

Finally, there may be instances whereby a user raises a request with the ICT Helpdesk Team to manually override a website's category as it may have been classified under a category to which it doesn't belong. The checkpoint three-tier architecture has been configured to automatically block all the categories of websites that are known to be highly malicious or which could offend views, such as websites that may have adult or sexually explicit material and potentially offensive content, hacking sites or security exploitation sites, illegal substances, violence, intolerance and hate, gambling and gaming, etc.

Backups and off-site storage

Backing up of data is considered as one of the information security best practices that has gained increased relevance in recent years. It is thus essential to have a proven system backup strategy that creates backup copies of the organisation's IT systems from which an IT administrator can roll back in case of a disruptive event. This might include a simple restore of lost or corrupted data or a full system restore, due to a hardware malfunction, or a complete loss of computer operations because of fire. Nowadays, with the advent of ransomware, having a full, current and tested backup of your data can be a lifesaver.

The PA's ICT section has adopted a backup strategy on all its servers with a mix of incremental, differential and full backups. A dedicated backup software application was installed and configured to manage all the backups and recovery of data. The backups are monitored on a daily basis, to ensure that the daily/weekly/monthly backups are completed successfully. In the event that a specific backup has failed, the ICT Helpdesk Team will raise an incident request on JRIS and escalate the incident to the Network and PC Support Team to establish the root cause of failure and decide if a manual backup should be taken.

The NAO was also informed that the backups are either saved on a Network Attached Storage (NAS) device or on tapes. In the case of backup media, these are stored off-site in a fire resistant safe, which is kept in a locked room and access to this room is given to authorised personnel only by the security personnel at the off-site location.

Finally, if a file, folder or a system restore is required from backups, an incident request is once again raised by the ICT Helpdesk Team and the incident is escalated to the Network and PC Support Team to restore the requested file/folder or system from the related backup accordingly.

2.5.3 Risk Management

Risk management is designed to reduce or eliminate the risk of certain kinds of events happening, which may impact the organisation. This requires the identification, assessment and prioritisation of risks of different kinds. Once the risks are identified, a plan is drawn up on how to minimise or eliminate the negative impact of such events.

In view of the above, an organisation must carry out a risk assessment to analyse the value of its assets, identify possible threats to those assets, and assess the level of vulnerability to those threats. Instances like fires, floods, hardware/software failures, virus attacks, DoS attacks, cyberattacks and internal exploits are all examples of the types of threats that are to be analysed, and assigning a probability assessment value to each.

Once a risk assessment has been completed, the next step is to carry out a business impact analysis, which is an analytic process that aims to reveal business and operational impacts stemming from potential incidents or events. This process should lead to a report listing the likely incidents and their related business impact in terms of time, resources and money. Such a report should provide a clear understanding of the impact of non-availability of the IT systems and how this will affect the '*modus operandi*' of the organisation. In addition, an organisation should also list and review its critical and non-critical functions, and for each critical function, determine the:

- Recovery point objective – the acceptable data loss in case of disruption of operations. It indicates the earliest point in time in which it is acceptable to recover the data.

- Recovery time objective – 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 risk assessment and business impact analysis are finalised, the organisation would then be in a position to draft a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) at the organisational level.

A BCP defines the roles and responsibilities and identifies the critical IT application programs, operating systems, networks personnel and system administrators, 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.

A DRP, on the other hand, refers to the process of rebuilding the operations or infrastructure following a disaster. The DRP is a key component of a BCP, which includes the advanced planning and preparations necessary to minimise any loss and ensure continuity of critical business functions in the event of a disaster. Thus, a DRP comprises consistent actions to be undertaken prior to, during and following a disaster.

2.6 Observations, Conclusions and Recommendations

2.6.1 ICT Strategy

Whilst the NAO acknowledges the fact that the PA does not have a formal ICT strategy, the NAO commends all the initiatives undertaken by the PA over the past few years. However, the NAO highly recommends that the PA embarks on drafting a formal strategic plan for the coming years. This would serve to document the link between the objectives of the current ICT three-year plans and the objectives of the PA's strategic plan.

2.6.2 ICT Budgeting

The NAO recommends that the PA draws up a policy that would require that a written business case is submitted for review, at the Director's meetings, for each proposed major ICT investments. This policy should also include a template for such a business case.

Furthermore, the NAO also recommends that minutes of the Director's meetings with the Executive Chairman are taken, especially those meetings where:

- Changes that may impact ICT operations are being discussed.
- Business cases for ICT investments are being assessed.

Such minutes would serve as a written record (for audit purposes) of the rationale used in determining the need for a proposed ICT related investment/change and the process used to review the options considered.

2.6.3 Disposal of ICT equipment

As stated earlier in the report, the last disposal of assets was carried out five years ago, whereby a sub-contractor was engaged to dispose of ICT equipment, which was obsolete or beyond economical repair. However, the PA could not trace any digital documentation related to the above-mentioned disposal of ICT equipment. The only digital records found were related to a number of working PCs and monitors, which were donated to charity in November 2018.

In the meantime, the NAO was informed that ICT equipment, which can no longer be utilised because it is either obsolete or beyond economical repair, is being put aside and stored for disposal until a large enough quantity is collected. Similarly, hard disks are removed from each device before disposal, and then they are dismantled, destroyed and disposed of separately. In this regard, the NAO recommends that when the PA decides to dispose of a number of obsolete or faulty ICT equipment, a sub-contractor is engaged and ensure that the PA keeps a record of all the items disposed of in the Hardware Inventory system application. In terms of hard disks, the NAO also recommends that these are physically destroyed (shredded) through a third-party operator, and the PA oversees the shredding process of hard disks. Upon completion, the operator should then provide a '*Certificate of Destruction*' that will include the number of hard disks that were shredded on that date.

2.6.4 Patch Management

Notwithstanding that the Windows servers and Microsoft SQL server instances are being updated regularly with the latest hotfixes and security patches, the NAO recommends that these should ideally first be installed manually on a test environment. If no abnormal behaviour is observed, these hotfixes and patch releases must then be deployed on the 'live' servers.

2.6.5 Risk Management

The NAO was informed that notwithstanding that the PA had incidents of non-availability of IT systems in the past, which might have impacted its overall operation, the PA has never conducted a business impact analysis or a risk assessment exercise, and thus, the PA does not have a BCP and DRP in place.

In this regard, the NAO was informed that the PA obtained funds from an EU funded project for consultancy on drafting a BCP and DRP, which will also include a risk assessment exercise. The project, entitled '*Support for the study regarding distributed ledger technology (DLT), security analysis, business continuity and disaster recovery plans*', kicked off in February 2020 with an introductory meeting. It is envisaged that through this project, the PA would be in a position to further embrace new digital technologies and get in line with the European Digital Agenda. At the same time, the PA would further align itself with Malta's National Reform Programme (April 2018)[15] of which the country's ICT agenda is an integral part of it.

In this regard, the NAO noted that one of the objectives that the PA will be focusing on during this study is to '*identify critical resources, risks and points of failure and the drawing up of ICT business continuity and ICT disaster recovery plans in relation to Information and Communications Technology*'. As part of this study, a number of workshops have already taken place, including workshops related to '*network security and systems architecture*' and '*ICT related BCP and DRP*'. More workshops have already been scheduled till February 2021, covering topics such '*Blockchain and DLT*' and '*BRP and DRP*' amongst others.

The NAO is of the opinion that following this study, the PA would be in a better position to draw up a risk management strategy, on the various topics highlighted above, and be able to implement it across the PA, to ensure that the Authority would be able to identify, assess and manage any type of ICT related risk, and draft a BCP and DRP at an organisational level.

[15] https://mfin.gov.mt/en/Library/Documents/NRP/NRP%202018.pdf

Chapter 3

ICT Systems

During the course of this IT audit, and as mentioned earlier in Chapter one, the NAO has reviewed the core IT software applications in use within the PA, namely:

- Artemis
- eApplications
- Billing and BLC

3.1 Artemis Application

The Artemis application was launched in August 2010, running in parallel with the existing Acolaid software application, whilst still making use of physical files. By January 2016, the PA completed the shift from the Acolaid software application to the Artemis software application, which has since been in use by all the PA's Directorates. This changeover was necessary not only to eliminate the fragmentation of information, but also to eliminate the resultant duplication of work involved through the inputting and maintaining of information in the previously utilised electronic and manual systems.

The shift from using the 'old' Acolaid software application and manual files with the introduction of the Artemis software application has resulted in the centralisation of all documentation related to development applications, thus improving communication between PA Directorates, whilst multiple processes could be performed concurrently, thus making the process more efficient. Although the disadvantages associated with the handling of manual files have been eliminated, the PA stated that physical documents may still be accessed when reviewing documents related to major projects.

The Artemis application is nowadays being used by all the PA officials to: record all the relevant information for the processing of applications; view the documentation (ex. site plans and photos) submitted online by the architects, consultees and external stakeholders through the eApplications portal; generate and send any other documentation to external stakeholders; and communicate internally between the PA's Directorates. In addition, the Artemis is also used for the recording of information and documentation relating to enforcement cases.

For the purpose of this IT audit, the NAO reviewed how the Artemis application is being used by different PA officials for the processing of planning applications, which are submitted online by the architects through the eApplications portal, and the way the ICT section manages the Artemis application in terms of maintenance and support.

The Artemis application is hosted on a virtual environment that is installed on a physical server housed at the PA's server room. This server is also replicated on another physical server at the PA's disaster recovery site as a countermeasure in the event that the physical server at the PA's server room malfunctions. In this regard, the ICT section is monitoring and maintaining the upkeep of these servers (including the virtual environments installed on each server) to ensure that both servers are backed up on a daily basis.

The Artemis application is integrated with the PA's AD domain and thus all the user accounts will inherit the same security settings in terms of user authentication, password policies and the resources that users are permitted to access amongst others. Thus, the same account credentials that are used for a user to log on to his/her workstation on the PA's domain are applied again when logging on to the Artemis application. If a user has forgotten his/her password, the user must request a password change, whereby a random password is generated and sent to the user via SMS to his/her personal phone. If the user does not have access to their phone, they must physically go to the Networks and PC Support Team's office to collect their newly generated password. Every new password generated must be changed again upon first logon, and the password must be set with a minimum number of characters, letters and numbers. In addition, the NAO noted that previous passwords are not allowed, and every password is set to expire over a period of days.

The NAO observed that a user may be assigned multiple roles within the system, and for each user and/or workflow groups to which the user is assigned, a to-do list is displayed on screen upon logging on to the Artemis application. The to-do list[16] depicts a number of cases (or applications) and the necessary actions the user is required to take for each of these cases/applications. These are created after other sections from within the PA have finished working on the case/application from their end and may be directed to a specific user or other sections depending on the pending action item required.

When a new application is submitted online through the eApplications portal, the application can be viewed in real-time on Artemis. In turn, each application goes through a number of stages, in which a number of checks are made, before a decision is taken whether the proposed development is granted, granted with certain imposed conditions, or refused by the PA.

At the initial vetting stage, PA officials have to go through each and every application submitted online, and ensure that all the mandatory fields were inputted correctly, and the documentation requested for the proposed development, such as fully dimensioned drawings, site plans and good quality coloured photos taken from different angles, are clear enough to print without loss of

[16] The to-do list is also created when external users interact with the PA through the eApplications, for instance, when the Architects upload new plans, consultation replies, etc.

detail. The NAO noted that most of these checks are carried out manually, but the system was developed to facilitate the process through a number of system checks. Thus, if for instance the email address of the applicant is similar to the architect's email address, the system will trigger a notification that the two email addresses are the same. The architect may also be requested to submit further information, such as a clearance letter from the Lands Authority which must be submitted when development is carried out on Government owned land. If the letter is not submitted, the PA official reviewing this new application will make a note on Artemis showing that the PA is still awaiting the Lands Authority's clearance letter from the architect.

Meanwhile, all the missing documentation requested by the PA must be submitted by the architect within three months from being notified (following vetting), before the PA could proceed with the processing of the application. In this scenario, both the architect and the applicant are informed by email, and all correspondence is automatically recorded in Artemis under the *Minutes* tab. If the documentation is not submitted within the stipulated three-month timeframe, the application submitted online is automatically withdrawn from the system.

Following the initial vetting stage, the application goes through the next billing stage. It is to be noted that a bill cannot be issued unless all the required information/documentation has been submitted. As such, the quicker the full information/documentation is submitted by the architect/applicant, the quicker the bill is issued. The bill is generated according to the Subsidiary Legislation 552.12 – Development Planning (Fees) Regulations[17] and is divided into the following main items:

- *Development Permit fee (DPF) and Environment fee*[18] *– both the DPF and Environment fee are the fees to be paid in respect of an application for permission to carry out development at the rates set out in Schedule 1, Categories A, B and C. The rates set out in Schedule 1, Categories A, B and C shall be subject to a minimum development permit fee of €120.*

- *Street contribution and Sewer contribution*[19] *– these are referred as infrastructure services contribution. The fees charged to the client are based upon the rate of contribution to be paid towards the cost of infrastructure services and other services, or facilities arising from any permission to develop land. These fees are passed on to Transport Malta (Roads Department) and the Water Services Corporation (Drainage Department) respectively.*

Once the bill is settled, the initial vetter is informed through a minute in Artemis. In turn, the initial vetter would then be in a position to validate the application and issue the PA number. However, there may be instances whereby a revised bill is required following further input/changes by the

[17] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=11575&l=1

[18] The rates are based upon the "Payment of Development Permit Fee and Environment Fee. Substituted by: L.N. 126 of 2013"

[19] The rates are based upon the "Development Planning (Fees) Regulations, 2010 - L.N. 356 of 2010"

Case Officer, within the PA, especially when new information/documentation submissions are made, usually in relation to some minor amendments to the original application requested by the architect/applicant.

Following the above, the application goes through the Plotting stage, whereby a PA official utilizes the Geographical Information System (GIS)[20], apart from the Artemis application, to plot the site extents of the proposed development, as submitted by the architect in the site plan, and check whether there were any previous permits on the proposed site and link them to the new proposed development application accordingly. In addition, the PA official must also verify that the proposed development is within the proper administrative (local council) boundaries, similar to what was submitted by the application in the initial stages. Following the above checks, the PA official can then assign the (newly plotted) proposed development application with the PA Case number (ex. PA/01234/19), the latter being the same number that was inputted on Artemis following the initial vetting stage.

Once all the work (plotting) on the GIS application is completed, the PA official saves it in *.pdf* format and manually uploads it on the Artemis application, as a new minute. The saved document, which is referred to as the site notice[21], is printed, and together with the site plans and relative photos are then fixed on site where the development is being proposed.

In the meantime, the NAO was informed that every Wednesday, the PA publishes a press notice on the Department of Information website (eventually published on the Government Gazette), which includes all the site notices that were issued during the prior week. The local councils are also informed electronically, listing the development applications pertaining to their locality. In turn, local councils are encouraged to publicize and maintain an updated list of such development applications accordingly.

The endorsement stage comes into play once the consultations have been concluded and the Case Officer has gone through the whole application process and submits the necessary recommendations in the form of a report. The Case Officer will prepare a small report in the case of a Summary Procedure Application (Schedule 2), whilst a full report will be prepared in the case of a Full Development Application. In either case, once the report is concluded, this shows up as a minute in the *Minutes* tab.

Legal Notice 162 of 2016[22] stipulates that a proposed development can be classified as a Summary Procedure Application (Schedule 2) or as a Full Development Application, each having their own differing target dates. Thus, when a Summary Procedure Application is submitted, the Chairperson of the Planning Board or his delegate must decide on the application within six weeks (42 days) from

[20] The GIS allows for the selection and combination of different data sets including the development boundaries (between towns and villages), planning and base data, scheduling and enforcement notices.

[21] Once the site notice is affixed, the applicant is held responsible to ensure that the notice remains affixed on site for the period stipulated in the said notice. Meanwhile, an administrative fine may be imposed on the applicant for failure to retain the notice affixed on site for the period stipulated in the said notice.

[22] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=27682&l=1

the publication of the application, subject to the application conforming to all the requirements stipulated in the law. On the other hand, a Full Development Application goes into more detail and thus the Planning Board or its delegate must first review the application within 100 days from the publication date of the application.

Therefore, during the endorsement stage, the PA official reviews the report that was submitted by the Case Officer together with any submissions uploaded on Artemis in the *Minutes* tab, and then carries out various checks, depending on the type of application (Summary or Full), to ensure that the work done by the Case Officer is all correct.

At the end of this stage, the development may either be recommended to be granted, or granted with certain imposed conditions or refused[23]. In any case, the PA official must write down the reasons behind his/her decision, usually non-compliance with PA policies, standards or guidance in case of refusal, or granted with certain imposed conditions.

There may be instances whereby an application is approved, but the PA would impose some planning gains if for instance the developers cannot offer adequate on-site parking within their development, resulting in the loss of car parking spaces. When this is the case, the *Commuted Parking Payment Scheme (CPPS)* comes into force, which levies an amount on developers who cannot offer adequate on-site parking. The scheme was originally designed to raise money to be used to provide public parking spaces to cope with the additional demand. In this context, in 2018, the PA introduced a three-tier rate system[24] whereby the developer must contribute the following rates as shown in Table 1 below:

Under provision (car spaces)	The first 2	Between 3 and 9	10 and over
Rate/space	€2,500	€6,000	€9,000

Table 1 - CPPS 3-tier rate system (source PA Circular 2/18)

Apart from the CPPS, the PA had also introduced the Urban Improvement Fund (UIF), which provides for the levy of a fee, where the collected funds are used for the benefit of the community in particular developments, especially where the CPPS is not in force in certain localities. In this context, the UIF promotes the improvement and embellishment works in urban areas, such as landscaping, traffic management and other urban projects, which are considered beneficial to the wider community. The fund is made available for all local councils, Government agencies, NGO's or private individuals, but the proposals would need to be submitted through the respective local council/s where the initiatives are intended to be implemented.

In the above scenarios, the sum due is calculated from the Billing system and shown in Artemis, based on parameters inputted and the selections made by the PA official using the system.

[23] An application following the Summary Process cannot be refused. If the application cannot be approved, it needs to be referred to the Full Process Full Development Applications.

[24] https://www.pa.org.mt/file.aspx?f=B642B38645BBA0DD9D96877C555742A594C063E4A165498A

Once the application is duly processed by the Case Officer and the endorsement stage is completed, a Board meeting is scheduled through Artemis for Full Development Applications, whilst Summary Procedure Applications are decided by the Chairperson or his delegate without a sitting. In the former scenario, the system will automatically set the date within the target 14 days (to allow for all parties to prepare and schedule accordingly) and a notification of the Board sitting date is communicated through the eApplications. The NAO observed that during the Board meeting, a member of the committee or the Chairperson him/herself will input all the decisions taken and the conditions imposed on the developers directly on the system. This will facilitate the process for other PA officials who want to view the decisions taken and take the necessary actions (ex. request the architect/applicant to submit further information or remind them to submit any bank guarantee for instance).

All the decisions taken by the Board (which are valid for five years from date of publication) are made available to both the architect and the applicant. In addition, a non-executable full development permit together with all the relevant documentation is printed and sent by mail to the applicant. Once all the pending documentation requested by the PA Board is submitted by the architect, and any pending fees are settled by the applicant, the PA would then be in a position to issue an executable full development permit. The latter is also printed and mailed to the applicant, whilst a soft copy is sent to the architect through the eApplications.

Finally, the NAO was informed that five days prior to the commencement of a development, the applicant must fill in a *Commencement notice form (PA 1/19)*[25] and inform the PA of the intention to carry out the necessary works as defined in the permit. Failure to fill in the Commencement notice or submit it within the stipulated timeframe, shall result in the imposition of fines according to *Schedule D of LN 277 of 2012*[26] or its amendments or its replacements.

The NAO was informed that since the PA was setup in 2016, it processed 39,056 applications (Table 2[27] refers) of which 34,169 applications were approved, 1,706 were not approved, whilst 1,234 were withdrawn by the architect/applicant. The total number of 1,948 applications, which were marked as pending, were eventually processed the following year in each case.

Year	Permitted	Not Permitted	Pending	Withdrawn	Total number of applications
April-December 2016	5,865	394	36	162	6,457
2017	9,909	466	64	298	10,737
2018	10,634	485	198	428	11,745
2019	7,760	361	1,650	346	10,117
	34,168	**1,706**	**1,948**	**1,234**	**39,056**

Table 2 - Processing of applications (source PA – May 2020)

[25] https://www.pa.org.mt/file.aspx?f=AD1986967DAAAAE19BBBA811756F46D5B6F348DF9465498A

[26] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=23630&l=1

[27] A snapshot showing the status of applications received as at May 2020

In terms of audit trails, the NAO noted that the Artemis application has a full audit trail functionality whereby the IT system administrator can easily view any changes made, who made the change, their role assigned within the system, the workstation from which the change was made. In addition, the 'old data' and the 'new data' are clearly displayed together with any details written in the *Comments* field. Anything submitted relating to an application, whether it's an email correspondence or documentation, can also be viewed from the *Minutes* tab.

Finally, since the Artemis application was developed in-house, the NAO noted that the ICT section maintains various documents for each application. Any modifications or enhancements made in the system, are clearly documented using different colour codes, and the text is struck through to easily view the changes that were made. In addition, the NAO was informed that the source code is being kept in a centralised location and is restricted to a limited number of users only. In the meantime, if errors are encountered while using the system, these are reported and logged in the JRIS application. In turn, the Application Development and Support Team from within the ICT section, would then see to these errors and try to find a solution within a reasonable timeframe.

3.2 eApplications Portal

As highlighted earlier in the report, (Section 2.2 refers), the PA has introduced an efficient and cost-effective ICT approach, whereby the processing system of each planning application is nowadays totally paperless, and all the applications are being submitted and managed online. To further improve on the functionality offered to external users, a complete overhaul to the original eApplications portal, was developed in-house by the ICT Unit and was launched in the beginning of 2017. In this regard, the NAO was informed that 34,685 applications were submitted online (Figure 1 refers) since the updated eApplications version 2.0 (eApps2) portal was launched.

During the IT audit, the NAO reviewed how the eApplications portal is being managed by the ICT section, and how it integrates with other software applications in use within the PA.

The eApplications portal is integrated with the Artemis application and can be seen as the frontend application for all the stakeholders and the general public, whilst the Artemis application is the backend application used by all the PA users to manage all the applications submitted online. The eApplications portal thus provides access to electronic documents and plans on planning applications and notifications. Architects and lawyers can submit applications, whilst any eID holder may submit correspondence related to planning applications. In addition, consultees can review documents and drawings that were uploaded online and submit their consultation replies related to planning applications. The PA may upload monitoring reports and it is envisaged that the submission of certain correspondence will be extended to other professionals who have been granted access to this portal, such as warranted engineers.

The NAO was informed that the eApplications portal is also hosted on a virtual environment that is installed on a physical server housed at the PA's server room. The physical server is also replicated on another physical server at the PA's disaster recovery site as a countermeasure in the event that the physical server at the PA's server room malfunctions. In this regard, the ICT section are monitoring and maintaining the upkeep of these servers (including the virtual environments on each server) and ensuring that both servers are being backed up daily.

Whilst reviewing the eApplications portal, the NAO observed that this portal is only accessible through a valid eID[28] account as per *Legal Notice 162 of 2016*[29]. When a user, with a valid eID account, logs on to the eApplication portal, the user can apply for a new role. This feature is only applicable if the user is an architect or a lawyer by profession, in which case the user must ensure that the contact details are correct and must also upload a copy of their warrant so that the PA would be in a position to process their application. Consultees, on the other hand, are nominated on behalf of the organisation that they are representing and are added manually in the system by the PA to ensure adequate control. The organisation must also contact the PA to remove their respective delegates, when these individuals are no longer employed with the respective organisation. Architects may manage their delegates directly through the system.

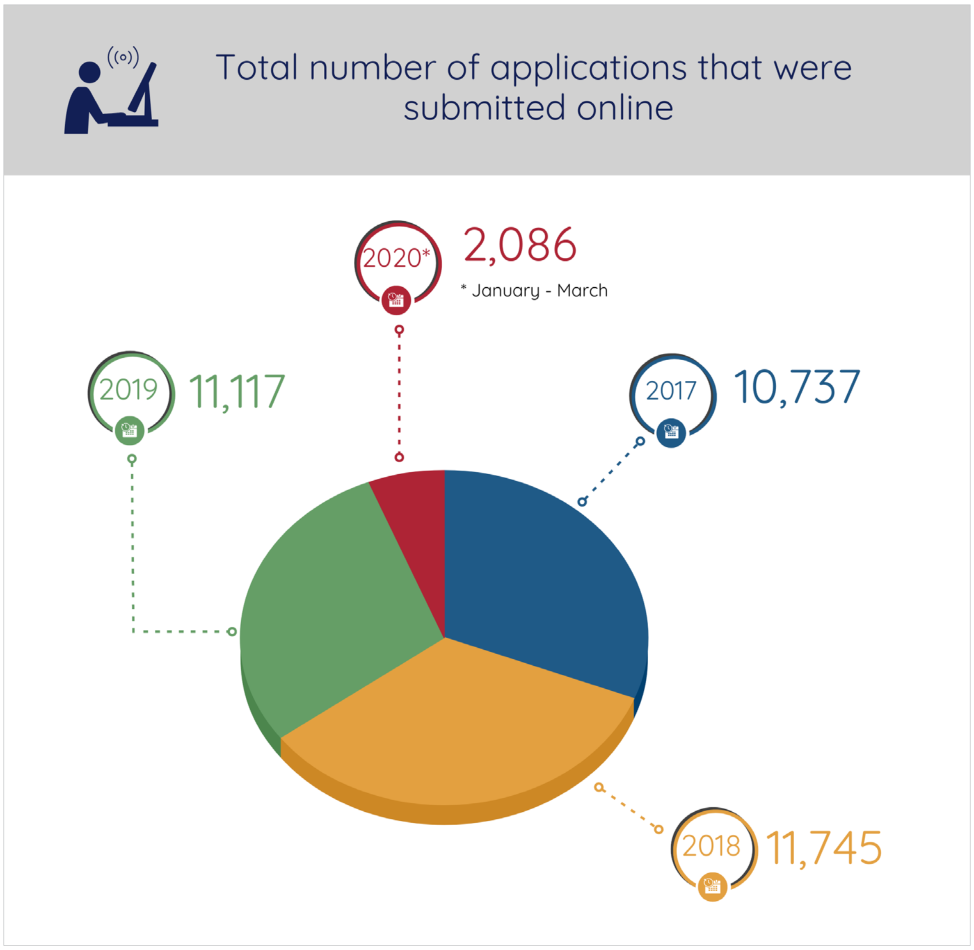


Figure 1 - Total number of applications that were submitted online (source PA – May 2020)

[28] An eID or electronic identity, is a trusted mechanism for Maltese citizens and businesses to identify themselves to electronically access services from across Government. The eID is issued by Identity Malta to any Maltese citizen or eResidence document holder who is over 14 years of age.

[29] All new applications must be submitted online through the eApplications portal and thus manual applications are no longer accepted by the PA.

Upon logging on to the system, a to-do list (ex. to provide further documentation or queries related to an existing application) is automatically displayed on screen in relation to all the previous applications submitted by the architect, and based upon actions/work and feedback from PA officers or other stakeholders working on a particular application. This list can be exported and saved in more detail in a *.csv* file, so that the end user (in this case the architect) could filter the list accordingly.

When submitting a new application, the architect must go through a number of steps and fill in the mandatory fields, such as the applicant details (it must be ensured that the name, surname, address, contact number and email address of the applicant are inputted correctly), the location of proposed development (the exact location where the development is being proposed must be submitted) and the documents to be attached (whenever there is a new application for a proposed development, the architect must submit various plans and photos) amongst others.

When compiling the application, the architect has the option to mark the application as '*Confidential*' in which case all the drawings that are uploaded will be automatically tagged as '*Confidential*'. This is in accordance with *Article 33 (2) of the Development Planning Act*, which stipulates that '*the application report and any plans concerning applications which relate to national security, defence, banks, prisons, the airport and other institutions or premises whose security it is desirable to safeguard as the Authority may establish shall not be made accessible to the public*'.

After filling in all the mandatory fields, the architect is directed to a payment page, and must pay an initial fee of €50 to proceed with the application with the PA. In terms of online payments, the NAO was informed that the PA utilizes the Government's Payment Gateway (GPG) through MITA's online services. Once the initial payment has been made, and the application is submitted, all the information can be viewed in real-time on the Artemis application.

As highlighted above, since the eApplications is the frontend of the Artemis application to the external stakeholders, everything is being recorded at the backend of the Artemis application, whether it's a new document that is uploaded, a new correspondence submitted, or a change in an existing field (ex. a change in the house number or email address). From the backend, the PA officer can view all this from the *Minutes* tab. On the other hand, if for instance, an end user opens a document, the eApplications will record who opened/accessed the document, and the date and time when this took place.

The NAO also observed that the eApplications portal has a sound searching functionality whereby the end user could easily search for previous applications and view related drawings/documentation submitted online. Thus, to search for a specific case, the end user must click on the search icon, select the type of case from a drop down list, for instance PA (Planning Application) or DN (Development Notification Order), input the 5-digit case reference number and the year when it was issued.

As stated in the previous section, since the eApplications portal was also developed in-house, the NAO noted that the ICT section maintains various documents for each application. Any modifications or enhancements made in the system, are clearly documented using different colour codes, and the text is struck through to easily view the changes that were made. The source code of the eApplications is also being kept in a centralised location and is restricted to a limited number of users only. Ever since the system was launched, the ICT section had only one instance in which they had to revert to a previous version of the application, due to an incompatibility with a *.dll* functionality when opening a *.pdf* file. In the meantime, if errors are encountered while using the system, these are reported and logged in the JRIS application. In turn, the Application Development and Support Team from within the ICT section, would then see to these errors and try to find a solution within a reasonable timeframe.

Finally, the NAO was informed that whilst the PA are currently using eApps2, it is envisaged that by the end of Q3 2020, the eApplications version 3.0 (eApps3) will be launched and shall be compliant with the web accessibility directive[30] by September 2020.

In this context, the NAO was informed that eApps3 will include major changes to the current frontend to make it more intuitive and more user friendly. For instance, the menus on the side will be discarded and instead the new interface used will be like that of a tablet. The end user could also arrange part of the interface to his/her liking, whilst the application forms will be re-designed and easier to use.

3.3 Billing and BLC

The BLC is the software application used to calculate and determine the relevant monetary fees due on a PA application, depending on the specific use/s and site floor area[31]. Fees generated from the BLC relate to Development Planning Application fees, which vary according to the development type, and include fees concerning Development Permit, Environmental Contribution, and Infrastructure Services Contribution for Street and Sewer.

Meanwhile, other fees/fines are generated directly from the Billing system, post Board review decision, relating to CPPS, UIF, Planning Gain, Sanctioning and Other Offences, amongst others, all of which are generated directly by the PA users.

Upon calculation, fees/fines generated (from either software) are automatically saved in relevant PA database, whilst using the Billing system to automatically generate the bill, record and store it, and send a copy to the applicant. Conversely, the payment receipts for the same bills, as well as any credit notes, are also issued from, recorded and hosted in the Billing system's database.

The Billing and BLC application is also linked to the Artemis system, whose backend database is also updated with some of the Billing and BLC data. Artemis users are also notified when a bill payment has been recorded.

[30] https://www.mca.org.mt/webaccessibility

[31] Applicable fees and calculations as per S.L. 552.12.

The Billing and BLC system runs on a Microsoft SQL server backend. The BLC system frontend is windows-based software application, which is installed on PA workstations, whilst the Billing application is a web-based form, which can be accessed from a PA network-connected device.

The Billing and BLC system was fully developed in-house, including all its enhancements and upgrades, at the PA, and any system maintenance and/or enhancements are in fact handled internally by the PA's ICT section.

Similar to other systems developed in-house at PA, the source code of the Billing and BLC is being kept in a centralised location and is restricted to a limited number of users. In addition, the PA utilizes GIT source control software application to ensure that version control is always maintained, whilst allowing for the possibility of reverting back to previous source code, should this become necessary. Such a setup also provides an adequate level of security and protection against malicious manipulation and/or theft.

Also, in common with other systems at the PA, this system is kept on a virtual environment that is installed on a physical server housed at the PA's server room, which is then replicated on the PA's disaster recovery site, for added protection.

The NAO was informed that system functionality is well documented and available in various documents, although no user manuals are in place. In this regard, the PA stated that new users to this application are trained on-the-job, on a one-to-one basis, although this is also supplemented by internal workshops.

As at audit date, the application's billing functionality was used by 50 internal users, whilst the BLC had 10 internal users. During its review, the NAO observed that the Billing and BLC system is in use by various officers within the PA's Vetting and Billing Units, although the output of this application is visible in the Artemis application and thus to all its PA users. In this regard, the NAO was pleased to note the segregation of user roles within these two Units.

The NAO was informed that the application has three different user levels, segregating officers who have full access to bills and cash sales, from those who can only issue bills, and those who can only carry out cash sales. These roles and the relevant user accounts are administered by the PA's ICT section.

User access is controlled via integrated AD login and password, thereby ensuring that the latter (login and password) user credentials are subject to the applicable AD policies. In this context, the PA stated that a random password is generated and sent via SMS to the user's personal phone whenever a request for password change is made[32]. This password will then have to be changed by the user upon first logon, thus guaranteeing a further degree of user access control.

[32] In the unusual event that the user does not have access to his/her personal phone, he/she will have to personally collect the newly generated password from the Networks and PC Support Team's office.

In addition, the NAO also learned that when a user's employment has been terminated[33], the user's account in AD is locked, automatically blocking access to all other systems with integrated AD login as well. Still, in situations of long-term user absence, it is the HR Unit's remit to determine when to inform the ICT section of such absence, for the user account to be disabled, or temporarily disabled, since the former may have authorised arrangements for teleworking during the same period.

The NAO was informed that the Billing and BLC system records all generated bills, and only when a bill or calculation is regenerated, is the previous one superseded (replaced). Besides, none of the application's users can delete any records relating to the generated bills. This setup is in place to sustain an audit trail.

During our audit, the PA provided the NAO a brief run through of the typical application usage scenarios, highlighting the complete process to issue a bill from the system, to the recording of the payment transaction in the accounting package, thereby following a transaction from start to end. Principal usage scenarios include generation of the Initial fee; calculation and issue of bills for additional fees (including revised bills) during vetting; issue of post decision fees or fines; accessing and viewing pending bills; and the settlement/payment of such bills/fines.

Throughout this review, the NAO observed that this system has a considerable degree of automation built into it, with some fees being generated/calculated automatically, though others are still dependant on manual user input during some of the application processing stages.

Primarily an example of a system generated fee is the Initial fee, created upon submission of a new (online) application through the eApplications portal. Before the application is accepted, the fixed fee must be paid online, using the applicant's credit card details, prior to submission. A payment receipt will then be generated by the system. Both bill and receipt are recorded in the Billing system, and will also be visible in the Artemis application in the *Minutes* tab.

Further on the process, the BLC needs to be accessed to address the main purpose of this application, that of calculating fees due and issuing bills. For instance, this is accessed during the initial vetting stage, where, depending on the type of development application that is being proposed, additional fees are due by the applicant/architect, and a bill for these fees needs to be generated and recorded[34]. In this regard, the NAO was informed that the BLC is updated to reflect any changes in legislation, legal notices, policies or schemes, which were applicable locally at distinct points in time. The BLC applies the related edition of the above, according to the relevant planning application date of the application being processed.

The user uploads the case details in the BLC, using the unique case number, and is presented with the *Fee Calculator*. The *Use Type* (to choose the type of fees[35] relevant to the specific application) is then selected by the user and the measurements (the size of the site area, obtained from drawings submitted with the application[36]) are inputted. The system then calculates the applicable fees due

[33] Upon termination of user employment, the HR Unit is responsible for informing the ICT Helpdesk Team, who will in turn, log a job request on JRIS.

[34] A bill cannot be issued until all the required information/documentation has been submitted by the architect/applicant.

[35] Type of fees, namely, Development Permit fee (DPF), Environment fee (ENV), Street Contribution fee (STR), and Main Sewer Contribution fee (SWR). Applicable fees are dependent on the use type and site area (size) of development, and are set out in S.L. 552.12.

[36] Measurements are not submitted in numeric format with the application but are manually measured off the submitted drawings by PA officers.

for the *Use Type* entered, based on inbuilt rates and parameters hard coded in the system, whilst generating an itemised bill. At this point, the user has the facility to preview the itemised bill, together with the system's calculations/workings, and if satisfied, can proceed with printing the bill.

This action will result in the calculation sheet and the bill being saved in the Artemis application's database, with the fees due listed under *Fees Required* in *Fee History* within the *Case History* tab, and shown as a new minute in the *Minutes* tab. Meanwhile, a copy of the bill is also sent to the architect, as a to-do item visible through the eApplications, and to the applicant, as a *.pdf* attachment in an email.

The NAO noted that the above process is also applicable to the issuance of revised (updated) bills, as well as newly generated bills. Such revised bills may be necessitated, for instance, after submission of additional information/documentation (following a request by the PA officer vetting the application), in relation to a request by the architect/applicant for minor amendments to the original application.

In this context, following its' issue, an itemised bill (whether new or revised) can then be viewed internally by PA officers either through the Billing system (for authorised users), by accessing the *View Bill* webform, and entering the relevant bill number, or through Artemis (for all other officers within the PA).

In the meantime, any payment of due bills can only be recorded through the Billing system, from which a receipt will be issued. In this regard, the NAO was informed that the PA accepts bill payments through Internet banking[37], as well as by cheque or payment at MaltaPost offices. Furthermore, (foreign) applicants can opt to settle all bills (excluding the initial fee) by means of SEPA transfer using the PA's IBAN. For the purpose of recording a payment, the applicable bill number is entered in the *Bill Payment* webform in the Billing system, following which the payment details are inputted. During our review, it was observed that this webform also has the facility to mark payments by cheque or epos as such. The receipt can then be issued and printed from the Billing system.

Consequently, upon printing, the receipt is saved in the Artemis application's database (similar to the process with a new bill), where each fee type is listed as having been paid under *Fee History* within the *Case History* tab, whilst the receipt for payment is recorded as a new minute in the *Minutes* tab. Simultaneously, the receipt is sent to the officer who previously issued the bill, as a to-do item visible in the Artemis application, whilst also being sent to the applicant via email, as a *.pdf* attachment.

[37] Online payment via Internet banking is offered through all three main local banks (detailed instructions are provided on PA's website). Online payment using applicant's credit card details is only accepted in respect of the Initial fee.

Following payment, receipts of bills settled can be viewed by the PA officers in the Billing system (for authorised users), through the *View Bill* webform, after inputting the relevant details, or through Artemis (for the remaining PA officers). At this stage, application processing can proceed to the next phase.

Both the architect and applicant can also access saved *.pdf* copies of the calculation sheet, bill, as well as any payment receipts, generated by the Billing and BLC system, through the eApplications portal.

A different scenario was also highlighted, where a bill can also be issued directly through the Billing system. This is applicable/used for post-decision fees or fines and may only be issued by authorised PA officers. This is done through the *New Bill* webform in the Billing system. The user inputs the case number to load the case, selects the type of fee to be applied, and inputs the amount to be charged, and then prints the bill.

The same process, as previously indicated when issuing a new bill (from the BLC), will then apply, with the bill being saved to Artemis backend, whilst also being forwarded to both the architect and the applicant at the same time.

With regards to the recording of billing/payment transactions in PA's accounting software, the NAO observed that this process is not automated, and is carried out manually at regular intervals, subject to receipt of payment[38]. Details, including a tracking number from the Billing system, are recorded in the accounting package for reconciliation purposes.

In the meantime, in terms of reporting functionality, whilst the Billing and BLC system does not have an inbuilt report generator, however, *Devart dbForge Query Builder* is utilised with Crystal Reports, by the Operations and ICT sections, to connect to the system's backend SQL databases, to create and generate reports as necessary. Meanwhile, end users have access to the Crystal Reports viewer, providing them with the possibility of re-running previously generated reports.

In this regard, the NAO noted a report, which is used by the Billing unit, to track PA applications which have yet to be processed. This report depicts all the pending bills, listing the system generated tracking number, the application creation date, and the time elapsed since the application was (initially) vetted, amongst other details, whilst highlighting, in red, applications which are approaching the processing deadline. This report is used by the Unit to monitor their workload.

Finally, in terms of a business process re-engineering, whilst the NAO was informed that such an exercise has not been formally carried out, nonetheless, the PA asserted that they look into, and occasionally carry out, operational procedure/process enhancement, or automation, following a review of a process or a way of working.

[38] Revenue is recorded upon receipt of payment, and not upon the issue of the bill. Payments received through a SEPA transfer are recorded on a weekly basis. Payments effected online, through internet banking, and MaltaPost, are recorded on a monthly basis. Payments by cheque are recorded once cheques have been deposited, on a daily basis. All payments are recorded only after bank deposits have been confirmed.

3.4 Observations, Findings and Recommendations

3.4.1 Centralisation of data and integration of systems

The NAO is pleased to note that the IT setup at the PA is based on Artemis as the core system, which was fully integrated with the eApplications and the Billing and BLC systems. This has resulted in the centralisation of all documentation related to development applications thus improving communication between PA Directorates, as well as eliminating the disadvantages associated with the handling of manual files.

3.4.2 Business continuity of the core software applications

The NAO commends the fact that the core software applications reviewed for the purpose of this IT audit, were hosted on a virtual environment[39] that was installed on a physical server housed at the PA's server room. Furthermore, in line with best practices in business continuity, the NAO also observed that this server was replicated on another physical server at the PA's disaster recovery site, as a fallback should the physical server at the PA's server room malfunction.

3.4.3 Safeguarding the source code

In line with best practices, the NAO positively noted that the PA took the necessary measures to securely store the latest version of the source code of the core software applications reviewed. Furthermore, version control of this source code was also maintained, which is critical should rollback be required. Any changes to the source code are clearly documented and access to this source code is restricted to a limited number of users only.

3.4.4 User authentication

The NAO commends the fact that the PA has integrated both the Artemis and the Billing and BLC with the PA's AD credentials for user access, and thus the same security settings in terms of user authentication, password policies and the resources that users are permitted to access, amongst others, are applied. In addition, access to the eApplications portal is done through the eID credentials, which is a trusted mechanism for Maltese citizens and businesses to identify themselves to electronically access services from across Government.

[39] Some of the main benefits of server virtualization relate to hardware costs, server provisioning and deployment, disaster recovery, energy costs and productivity.

3.4.5 Audit trail functionality

The NAO was pleased to note that the core systems reviewed for the purpose of this IT audit had a sound audit trail functionality, where every step of the processing of the development application is recorded centrally in real time.

3.4.6 Streamlining of processes

The NAO positively noted that both the Artemis and eApplications have a to-do list, which depicts the cases (or applications) in hand and the related actions the user is required to take. The action items are created after other sections from within the PA have finished working on the case/ application from their end or following a submission from external consultees or case architect. These action items may be directed to a specific user or other sections, depending on the pending action item required.

3.4.7 Better use of social media platforms

With reference to the publication of the PA press notices on the Government Gazette, the NAO opines that the PA is not making best use of social media platforms available in this regard. Thus, the NAO recommends that the PA conducts a review of the communication channels used for the publication of the PA press notices, to make better use of existing social media platforms, for instance, the PA may negotiate with the local councils the possibility of publishing the development application notices in their locality on their website and/or official Facebook page.

3.4.8 Business process re-engineering

The NAO was informed that the procedure for a regular business process re-engineering has not been formalised on some of the core systems reviewed for the purpose of this IT audit. However, this does not exclude that informal reviews have been carried out. In line with the above, the NAO recommends that this process is formalised and focuses on areas such as the possible automation of the recording of billing/payment transactions in PA's accounting software.

Chapter 4

Document management relating to the Planning Authority's administrative functions

4.1 Introduction

Document management is dependent on IT systems which in turn are intended to facilitate document traceability. The availability of documents contributes to the Authority's corporate governance as it safeguards audit trails and consequently transparency and accountability.

Document retention at the PA is a two-pronged operation. Firstly, it deals with the core function of the Authority, namely planning related issues. The second aspect relates to the administrative arm of the PA. This review focused on the latter aspect due to concerns reported to the NAO by third parties and issues raised by the Information and Data Protection Commissioner regarding the PA's document retention procedures.

Within this context, this Chapter discusses the extent to which the PA:

1. adheres to internal document retention policies; and

2. employs formal procedures governing the maintenance of administrative related documentation.

This Office requested and received information from the Planning Authority regarding contracts entered with third parties during the period 2013 to 2019. The PA declared the extent of documentation maintained regarding a randomly selected sample of 15 out of the 81 contracts that the Authority signed with third parties[40]. In order to check the integrity of the PA's declaration of documentation availability, the NAO focused on six contracts whose value was documented to be in excess of €100,000 and which were either awarded through a tendering procedure or a direct order. It is to be noted that this audit is solely concerned with document management and consequently, evaluation or review of the cost-effectiveness of the sampled contracts, is beyond its scope.

4.2 A document retention policy is not formalised

Formal requests and interviews with senior officials within the PA revealed that the Authority does not have a formalised document retention policy. In the circumstances, officials within the Planning

[40] One of these files was included in the sample because of concerns raised by third parties to this Office.

Authority adhere to document management practices which evolved over time. The maintenance of documents becomes fragmented in cases where the Executive Chairman/Chief Executive Officer (CEO) retain documentation within the registry catering exclusively for this office. Additionally, other records are maintained by the departments carrying out specific functions.

4.2.1 Document retention is mainly dependent on practices which evolved over time

The absence of a formalised document retention policy implies that the Authority's officials, at all levels, have a degree of flexibility on document management. Officials are however guided by legal provisions concerning procurement. Such provisions mainly relate to procurement materiality and procedural aspects. These elements become critical at the various phases of contract management, namely the award, implementation, certification of deliverables and payment. As will be discussed in Section 4.4.1, this review did not elicit documentation confirming that these procedures were followed in two of the four direct order awards reviewed.

4.2.2 Document management is not a centralised function

Administrative documentation within the PA is fragmented. The Directorate for Corporate Services maintains a centralised documentation system. However, other departments also maintain additional parallel systems that specifically cater for their needs.

A case in point is the separate registry maintained by the office of the Executive Chairman/CEO. This registry is intended to maintain and safeguard sensitive documents which require the incumbent's endorsement. This review showed that in one out of the four cases reviewed, which related to direct order awards, the relative requests and approvals for these contractual arrangements as well as the engagement letters with third party were solely maintained by the office of the Executive Chairman/CEO.

This raises concerns related to the fragmentation and availability of documentation. Generally accepted practices outline the importance of maintaining an up-to-date catalogue of documentation throughout the whole organisation. The PA deviated from such practices since it did not maintain a comprehensive document management system. While acknowledging that there may be an organisational need to maintain separate filing systems, it remains imperative that the main registry, at the very least, maintains references and visibility to documentation filed in other locations within the PA. The non-availability of a comprehensive documentation management system raises the risk that documents will not be readily retrieved to the detriment of organisational continuity, transparency, accountability – components of good corporate governance.

4.3 The Planning Authority did not maintain all the relevant documentation pertaining to contract management in relation to some direct orders

The NAO employed a two-tiered random sampling approach. Document management is considered to be critical to an organisation where zero-tolerance is adopted. Consequently, there was no need for the NAO to adopt statistically representative sampling. The initial review of 15 cases, which was subsequently followed by more in-depth scrutiny of six of these cases, revealed a number of shortcomings as portrayed within this Section. Table 3 refers.

Case number	Internal PA reference number	Description of the Service	Cost as per contract (excl. VAT)	Year	Needs Analysis	Direct Order or Tender	If direct order, copy of approval from MFIN	Signed copy of Agreement
1	DO14/2017	Engineering Consultancy Services	€ 16,900	2017	Y	Direct Order	Y	No agreement was made
2	PCQ 10/2017	Pembroke Development Brief - Transport Impact Assessment	€ 18,800	2017	Y	Direct Order	Y	Y
3	T04/2017	Service Tender for a Media Train for Publicity and Dissemination	€ 24,910	2017	Y	Tender	N/A	Y
4	CT3074/2017	Service Tender for Dissemination Tool/s for the Distribution and Reporting of Data to the Government, Public, Scientific Domains and EU/ International Reporting	€ 145,000	2018	Y	Tender	N/A	Y
5	N/A	Provision of Technical Guidance for the preparation and the assessment of safety reports according to SEVESO Directive	€ 150,000	2016	N	Direct Order	Y	Cannot confirm the existence of an agreement or otherwise

Case number	Internal PA reference number	Description of the Service	Cost as per contract (excl. VAT)	Year	Needs Analysis	Direct Order or Tender	If direct order, copy of approval from MFIN	Signed copy of Agreement
6	DO05/2019	Provision of Restoration and Architecture Consultancy Services	€ 50,000	2019	Y	Direct Order	Y	Y
7	N/A	Undertaking Regular Benchmarking of MEPA's reputation	€ 117,000	2013	N	Direct Order	Y	Cannot confirm the existence of an agreement or otherwise
8	N/A	Consultancy services in Spatial Information Systems and Information for a period of 5 years	€ 100,000	2015	N	Direct Order	Y	Y
9	CT3007/2017	Service tender for the creation of a large-scale topographic base map of Malta as part of an Integrated Nation Mapping Strategy	€1,230,963	2017	Y	Tender	N/A	Y
10	N/A	Provision of professional services as an architect in charge of infrastructure and refurbishment works at Floriana - EPRT	€ 32,000	2016	Y	Direct Order	Y	N/A – applying fixed rate

Case number	Internal PA reference number	Description of the Service	Cost as per contract (excl. VAT)	Year	Needs Analysis	Direct Order or Tender	If direct order, copy of approval from MFIN	Signed copy of Agreement
11	T02/2013	Compilation of an Interpretation Manual for Marine Habitats within the 25nm fisheries management zone around the Republic of Malta	€ 11,850	2013	Y	Tender	N/A	Y
12	T03/2018	Tender for the Provision of Health and Safety Services to the Planning Authority	€ 43,661	2018	Y	Tender	N/A	Y
13	DO14/2018	Upgrade of PlotGIS System (Planning Authority GI Plotting System)	€ 75,000	2018	Y	Direct Order	Y	Y
14	N/A	Re-development of the DCGIS system	€ 88,000	2016	Y	Direct Order	Y	Y
15	DO19/2019	Formulation of a framework to compile a socio-economic heat map, to represent the demand and supply factors relevant to residential and commercial development in Malta and Gozo	€ 140,000	2019	Y	Direct Order	Y	Y

Table 3 - The preliminary phases of the procurement process (2013 – 2019)

Table 3 provides a snapshot of the 15 cases under review during the preliminary phases of the procurement process. For the purpose of this audit, this phase considers the identification that services were required up to the stage where the PA awarded the contract. This Table confirms that important components of document management were lacking.

4.3.1 A third of the 15 files were not assigned an internal reference number

Key to a document registry system is the file reference number. Such a system facilitates tracking of documentation pertaining to the same file and grouping of information under one heading. Thus, it facilitates audit trail and transparency. However, five of the 15 cases were not assigned an internal reference number. Table 3 shows that all of these cases were direct orders. This situation raises transparency concerns, in view that, apart from the lack of a file reference number, these services were awarded to specific parties without a call for tender.

4.3.2 Needs analysis documentation was sparse

The PA declared that all of the 15 sampled cases had undergone a formal needs analysis evaluation. On further review, it transpired that in the case of direct orders, the PA was interpreting the information submitted within the request for the Ministry for Finance (MFIN) approval as a needs analysis report. This interpretation of a needs analysis differs significantly from the formal and comprehensive evaluations undertaken by the Authority with respect to services procured through a call for tenders. The PA contended that case materiality influenced the scope of needs analysis undertaken and in cases these would have been discussed in various management fora. Nonetheless, all the sampled direct orders sought finance approval for values exceeding €100,000. The absence or narrowly scoped needs analysis hampers an organisation from appropriately fulfilling the principles of corporate governance since decision making is not complemented by a robust audit trail.

4.3.3 The Planning Authority could not always confirm the existence of a contract

Table 3 also shows that in three of the 15 sampled cases the PA either did not enter or could not confirm the existence of a contractual agreement. These cases related to the provision of engineering consultancy services, the provision of technical guidance for the preparation and the assessment of safety reports according to SEVESO Directive[41] as well as preparing a recurring market research exercise to assess the current and ongoing perceptions relating to MEPA. The collective approved value of these cases amounted to €283,900. This Office further reviewed two out of these three contracts as their estimated value exceeded €100,000 in each case.

Fulfilling the provisions of the SEVESO Directive, entailed that the PA procure services related to the assessment of safety of major infrastructural projects. In view of the specialised expertise

[41] https://ec.europa.eu/environment/seveso/

required, the PA was constrained to seek MFIN approval to procure such services through a direct order. The sampled case was the third in sequence of direct order awarded to the same supplier in a period of three years.

While not disputing the need to procure these specialised services through a direct order, this Office queries why the PA did not formalise the relationship with the supplier through a contractual agreement. To this end, the PA did not present documentation in this regard. Moreover, PA documentation shows that the three consecutive direct order awards were always carried out through an engagement letter rather than a contractual agreement. The engagement letter in question did not comprehensively establish the parties' obligations and did not define adequately the payment terms. This state of affairs deviates from the principles of corporate governance in terms of document and contract management.

This review elicited a second instance whereby the PA did not provide documentation relating to "*Undertaking Regular Benchmarking of MEPA's reputation*". Conversely to the previous case, the PA did not issue an engagement letter. Moreover, this review highlighted inconsistencies in the interpretation of events surrounding this case. The former PA Executive Chairman/CEO contends that the Authority entered into a formal contract with the supplier. On the other hand, the supplier notes that he never signed a formal agreement. According to the latter, the two parties signed a research brief/outline of the work to be performed. Such a copy was not available at the PA. However, the supplier provided a copy signed from their side relating to the first year of operation rather than for a three-year period.

4.4 The Planning Authority did not maintain all the relevant documentation pertaining to payment procedures in relation to the sampled direct orders

Documentation management pertaining to payment procedures is key to corporate governance. For the purpose of this audit, as shown in Table 4, the key steps reviewed within the payment procedures of the PA were:

1. sign-off of completed deliverables;
2. invoice related deliverables;
3. related payment; and
4. copy of receipt.

Case number	Description of the service	Copy of all invoices	Copy of the document certifying that works have been carried out according to specifications	Copy of internal approval for payment	Copy of payment including payment voucher	Copy of any correspondence exchanged between the two parties	Copy of correspondence exchange with third parties on the matter (Ex. complaints received/FOI correspondence)
1	Engineering Consultancy Services	Y	Y	Y	Y	Y	N/A
2	Pembroke Development Brief - Transport Impact Assessment	Y	Y	Y	Y	Y	N/A
3	Service Tender for a Media Train for Publicity and Dissemination	Y	Y	Y	Y	Y	N/A
4	Service Tender for Dissemination Tool/s for the Distribution and Reporting of Data to the Government, Public, Scientific Domains and EU/ International Reporting	Y	Y	Y	Y	Y	N/A

Case number	Description of the service	Copy of all invoices	Copy of the document certifying that works have been carried out according to specifications	Copy of internal approval for payment	Copy of payment including payment voucher	Copy of any correspondence exchanged between the two parties	Copy of correspondence exchange with third parties on the matter (Ex. complaints received/FOI correspondence)
5	Provision of Technical Guidance for the preparation and the assessment of safety reports according to SEVESO Directive	Y	Y	Y	Y	Cannot confirm the existence of any correspondence or otherwise	N/A
6	Provision of Restoration and Architecture Consultancy Services	Y	Y	Y	Y	N/A	N/A
7	Undertaking Regular Benchmarking of MEPA's reputation	Y	Y	Y	Y	Cannot confirm the existence of any correspondence or otherwise	Y
8	Consultancy services in Spatial Information Systems and Information for a period of 5 years	Y	Y	Y	Y	N/A	N/A

Case number	Description of the service	Copy of all invoices	Copy of the document certifying that works have been carried out according to specifications	Copy of internal approval for payment	Copy of payment including payment voucher	Copy of any correspondence exchanged between the two parties	Copy of correspondence exchange with third parties on the matter (Ex. complaints received/FOI correspondence)
9	Service tender for the creation of a large-scale topographic base map of Malta as part of an Integrated Nation Mapping Strategy	Y	Y	Y	Y	Y	N/A
10	Provision of professional services as an architect in charge of infrastructure and refurbishment works at Floriana – EPRT	Y	Y	Y	Y	Y	N/A
11	Compilation of an Interpretation Manual for Marine Habitats within the 25nm fisheries management zone around the Republic of Malta	Y	Y	Y	Y	N/A	N/A

Case number	Description of the service	Copy of all invoices	Copy of the document certifying that works have been carried out according to specifications	Copy of internal approval for payment	Copy of payment including payment voucher	Copy of any correspondence exchanged between the two parties	Copy of correspondence exchange with third parties on the matter (Ex. complaints received/FOI correspondence)
12	Tender for the Provision of Health and Safety Services to the Planning Authority	Y	Y	Y	Y	Y	N/A
13	Upgrade of PlotGIS System (Planning Authority GI Plotting System)	Y	Y	Y	Y	Y	N/A
14	Re-development of the DCGIS system	Y	Y	Y	Y	N/A	N/A
15	Formulation of a framework to compile a socio-economic heat map, to represent the demand and supply factors relevant to residential and commercial development in Malta and Gozo	Y	Y	Y	Y	Y	N/A

Table 4 - The payment procedure and correspondence exchanged relating to the 15 sampled cases

The NAO adopted a similar approach to the one utilised when evaluating document management relating to the preliminary phases of the procurement cycle. The PA declared that it maintained all key documentation relating to the payments with respect to the 15 sampled cases. However, on an in-depth review of six these cases, which were randomly selected and had a materiality exceeding €100,000, it transpired that in the case of direct orders, the documentation maintained by the PA was not comprehensive.

4.4.1 The Planning Authority did not always maintain certification of deliverables pertaining to direct order contracts

In two of the four direct orders which were reviewed in-depth, the PA did not maintain documentation certifying that deliverables were in accordance to the terms and conditions agreed with suppliers. These cases related to the "*Provision of Technical Guidance for the preparation and the assessment of safety reports according to SEVESO Directive*" and the "*Undertaking Regular Benchmarking of MEPA's reputation*".

In these two cases, certification citing the agreed specifications would not have been possible since there was no contract in place. Nonetheless, despite the absence of a contract, the PA did not draw up a document outlining agreed deliverables. Consequently, there is no audit trail to ascertain the quantity and quality of deliveries through these direct orders.

4.4.2 The Planning Authority does not appropriately vet invoices submitted by supplier prior to affecting payment

In one case relating to "*Undertaking Regular Benchmarking of MEPA's reputation*", the PA proceeded with payments even though the VAT number and company registration number quoted in the invoice did not pertain to the company awarded the direct order. Upon inquiry, PA stated that it does not routinely vet such details. Further enquiries with the Director of this company (who also endorsed the invoice) did not yield additional information on the matter.

The absence of such mechanisms within the payment procedures not only raises governance concerns but also increases the risks of illicit declaration or transfer of funds by third parties.

4.4.3 The Planning Authority did not maintain documentation in cases where contracts were terminated prior to their fulfilment

In one of the cases, according to the former Executive Chairman/CEO, the Authority terminated the contract after two months rather than at the envisaged juncture of 36 months due to unsatisfactory delivery. This Official's contention conflicts with the information furnished by the Director of the contracted firm who stated that the company felt that it had delivered the expected services and that there was no need to prolong the contract.

Conflicting statements is already a worrying fact, but matters are exacerbated as neither the PA nor the supplier furnished this Office with a termination letter. This deviates from generally accepted business practices and corporate governance principles. The PA documentation, however, shows that it honoured only the two invoices referred by the supplier for a total amount of €19,500. On this Office's request, the PA confirmed that further payments relating to this supply of services were not made to any of the other companies referred to in invoices.

4.5 Conclusions

This review of the PA's document management, specifically document retention, elicited mixed results. The main concerns relate to documentation pertaining to direct award cases. The sampled cases reviewed showed that, in cases where the PA procured goods and services through a tender process, the related documentation was adequate.

Conversely, the PA's document management, including its retention deviated from generally accepted practices in cases of direct orders. A case in point relates to the specific direct order where key documentation was also not made available to the requesting source in terms of the Freedom of Information Act. This review could not confirm whether the documentation was unavailable because it was either misplaced or not compiled. Additionally, this review noted two other cases where contracts relating to direct orders were not made available. Although one would expect that the PA would maintain the full documentation, the NAO sought to retrieve such documentation through other government entities but to no avail. This implies that the documentation may not have been drawn up at the outset. This raises concerns as to why the PA sought to adopt such procedures rather than apply the same processes as it did with the other cases.

It is clear that the PA needs to conduct a thorough internal review of its document management processes related to its administrative functions. It is critical that such a review considers the establishment of an organisation-wide document retention policy and complemented with the relative standard operating procedures. Previous Chapters of this Report acknowledged that the PA operates an efficient IT system handling permit applications documentation. Consequently, the situation portrayed in this Chapter is considered paradoxical as the administrative arm of the Authority does adopt similar documentation management procedures. The NAO recommends that the principles adopted for document management related to permit applications is applied to this sector of PA's business processes. This will strengthen the Authority's corporate governance in terms of transparency, accountability and efficiency.

Chapter 5

Management Comments

Subject: IT Audit: Planning Authority's reply to NAO's report

Reference is made to NAO's Audit Report on the Information Technology setup of the Planning Authority submitted via email dated 2nd September 2020. Discussions have been held by the undersigned with the Director Corporate Services and Director ICT, Mapping and Digital Services, and the following feedback to the report is being put forward:

With respect to the ICT Audit, the Planning Authority has decided to accept NAO's suggestion to compile and implement a three year strategy/plan based on the conclusions from the Business Continuity Plan and the Disaster Recovery Plan and any organisation strategy, business plans and objectives that the Authority may compile, from time to time. This strategy shall be presented to the Executive Council for approval before implementation.

Apart from the full justification required with respect to purchases exceeding €10,000 as per current Governmental procedures, the ICT Unit shall also be keeping a written justification for purchases exceeding €5,000 where requirement for such purchases need to be justified to the ICT Unit Manager and the Director, who shall review the requirement and endorse it accordingly. Such records shall be filed with our ICT Purchase Order filing system.

The Authority will also keep minutes of discussions held and decisions taken during Directors' meetings relating to all ICT matters including purchasing decisions and any ICT related actions required including time frames. These will be adequately retained for information purposes and communicated officially to the ICT Unit for action.

The PA has noted the NAO's suggestion relating to the disposal of ICT equipment and shall be taking this suggestion on board apart from instances where the PA decides to donate such equipment to charitable entities. In this case, an official receipt for the equipment, from the charitable entity receiving the goods, shall be sought.

In relation to Patch Management, the PA accepts the NAO's suggestion to create an adequate test environment to ensure that hotfixes and patches behave normally prior to being deployed to 'live' servers. However, it would like to note that it is not practical to have a full test environment of all the live servers, but a sample of similar servers will be created for such tests to be performed.

The NAO rightly pointed out that the PA does not have a formal risk assessment and as a result, no Business Continuity Plan and Disaster Recovery Plan. The Authority agrees and in fact was preparing these studies/plans in conjunction with a local consultant. Since the audit was undertaken, the risk assessment has been concluded and the Authority is finalising the BCP and DRP. As already mentioned, the PA would then propose a long-term strategy to the Executive Council based on the findings of such plans and will implement the same once officially approved.

The PA takes note of the NAO's suggestion to better utilize social media and as a result will consider providing a link on such media to the DOI webpage site relating to the publication of received and decided applications and is also in the process of recruiting PR assistance to advise on how to improve its presence on social media and assist in doing so with the aim of increasing the Authority's image and reach.

With respect to the section of the audit relating to document management relating to the PA's administrative functions, the NAO concluded that "in cases where the PA procured goods and services through a tender process, the related documentation was adequate" whilst in the case of two of the four direct orders making up NAO's sample, "the PA's document management, including its retention, deviated from generally accepted practices". The PA will take up NAO's recommendations and will undertake a review of its document management processes related to its administrative functions, which considers the establishment of an organization-wide document retention policy, which is complemented with the relative standard operating procedures.

The comprehensive documentation management system will ensure the centralised retention of all relevant documentation at the various phases of contract management, namely the preliminary needs analysis evaluation, the award, implementation, certification of deliverables and payment. These documents include the needs analysis template, tender documentation, supplier proposals and quotations, all the relative approvals and authorisations, contracts with suppliers, certification of deliverables, supplier invoices, payment documentation and receipts. The recommendation of assigning a unique internal file reference number to direct orders has already been put into practice as from January 2020, for direct orders having a value in excess of €5,000 excluding VAT. The checklist for invoice checking will be updated to include verification of VAT number and company registration number.

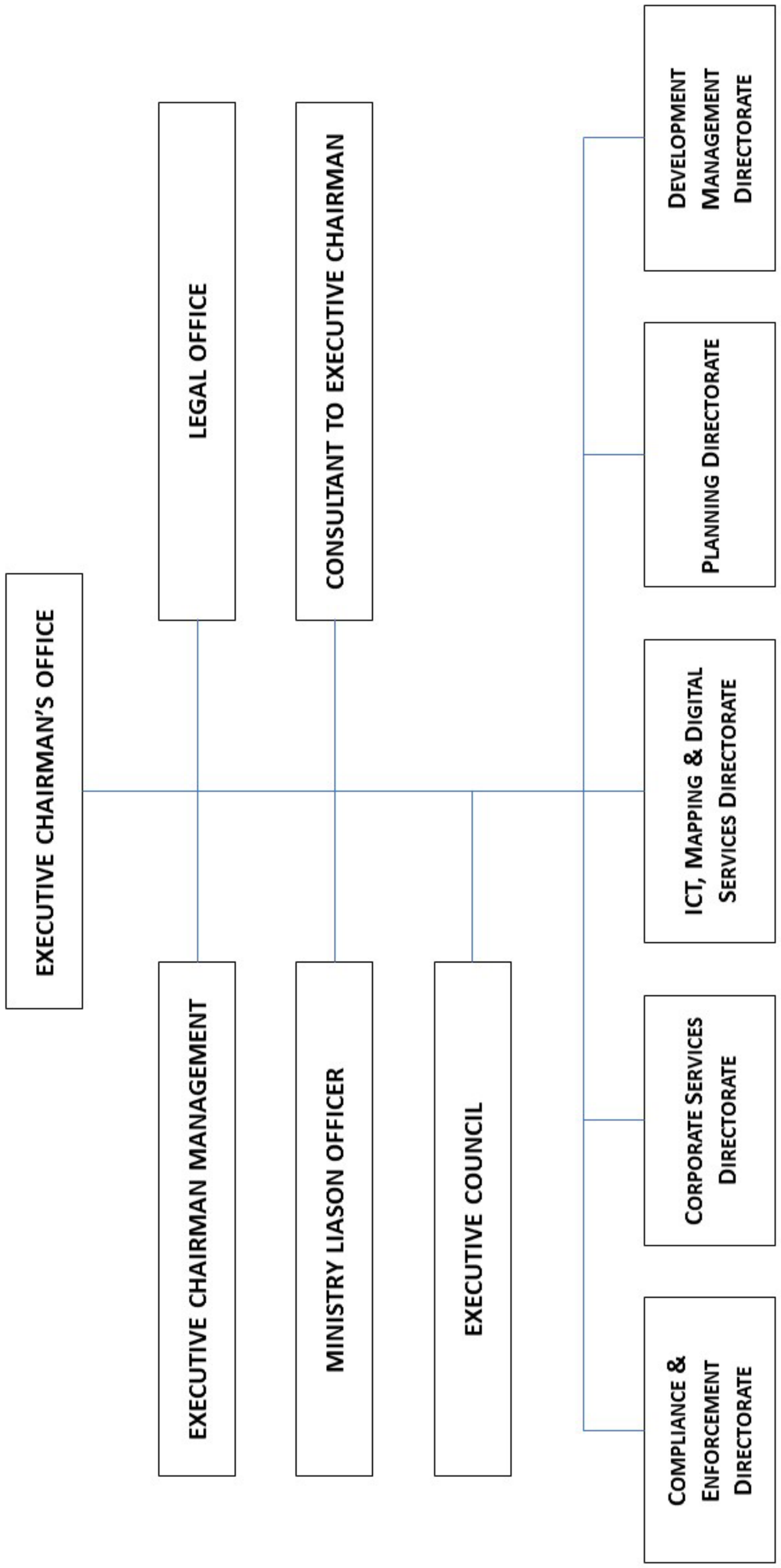
The PA will also be following NAO's recommendation to carry out and document a formal needs analysis evaluation for proposed major ICT investments. Business cases for ICT investments will be assessed at Directors' meetings, which will be duly minuted to serve as a written record for better governance. The PA will be drawing up a policy to this effect, which includes a needs analysis evaluation template establishing the rationale in determining the need for a proposed ICT related investment/change and the process used to review the options considered. The formal needs analysis evaluation template will also be adopted for any procurement in excess of €10,000 excluding VAT.

The undersigned wish to thank the NAO for the valuable work carried out as part of its review of the PA's document retention within the administrative function and for its recommendations to uphold the highest standards of governance within the Planning Authority.

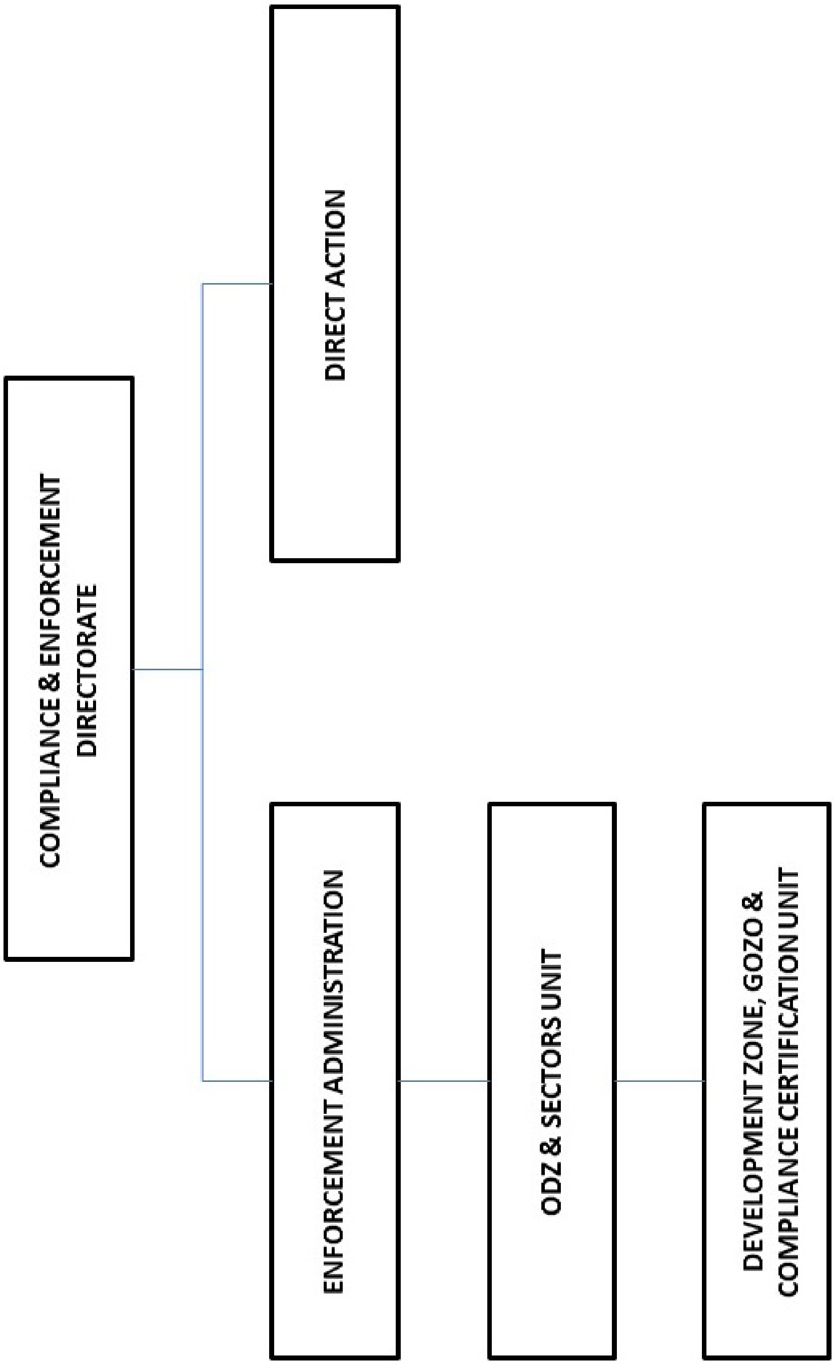
Martin Saliba
Executive Chairperson

15th September 2020

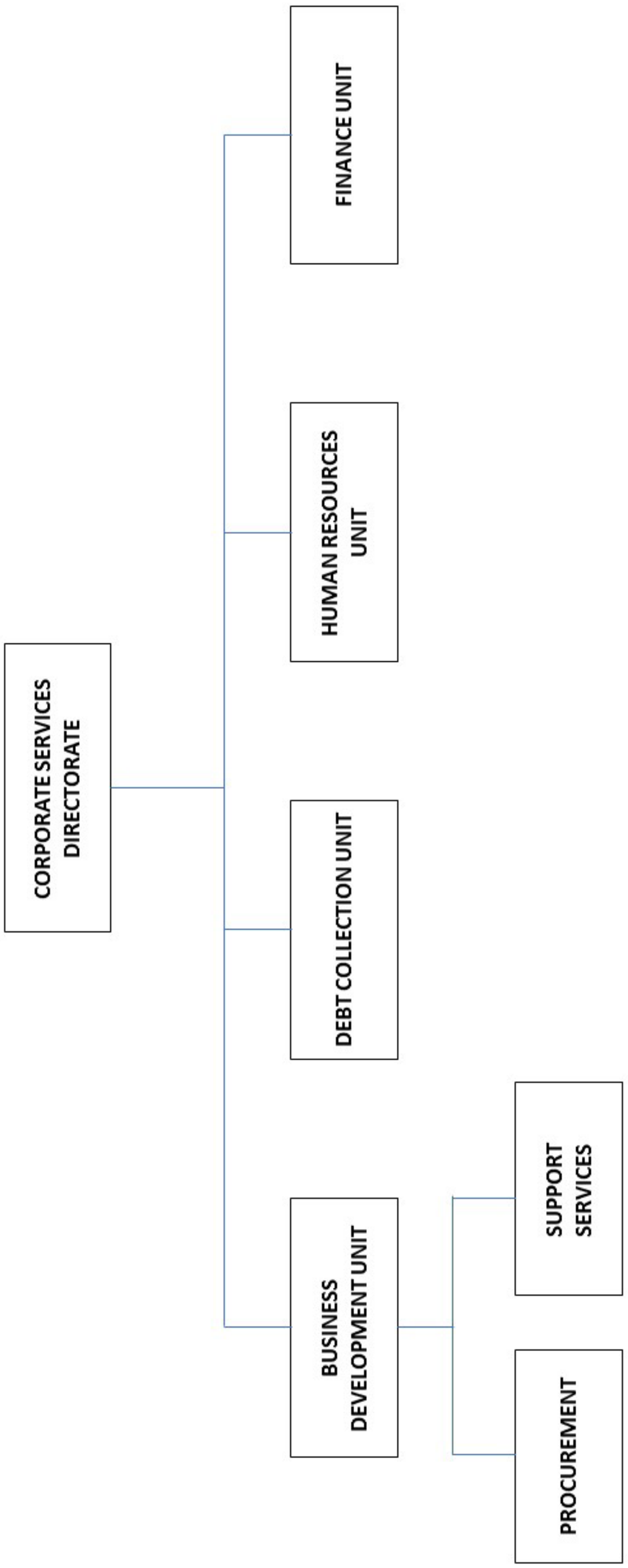
Appendix A: Planning Authority Organisational Charts


Executive Chairman's Office
Executive Chairman Management
Legal Office
Ministry Liason Officer
Consultant to Executive Chairman
Executive Council
Compliance & Enforcement Directorate
Corporate Services Directorate
ICT, Mapping & Digital Services Directorate
Planning Directorate
Development Management Directorate

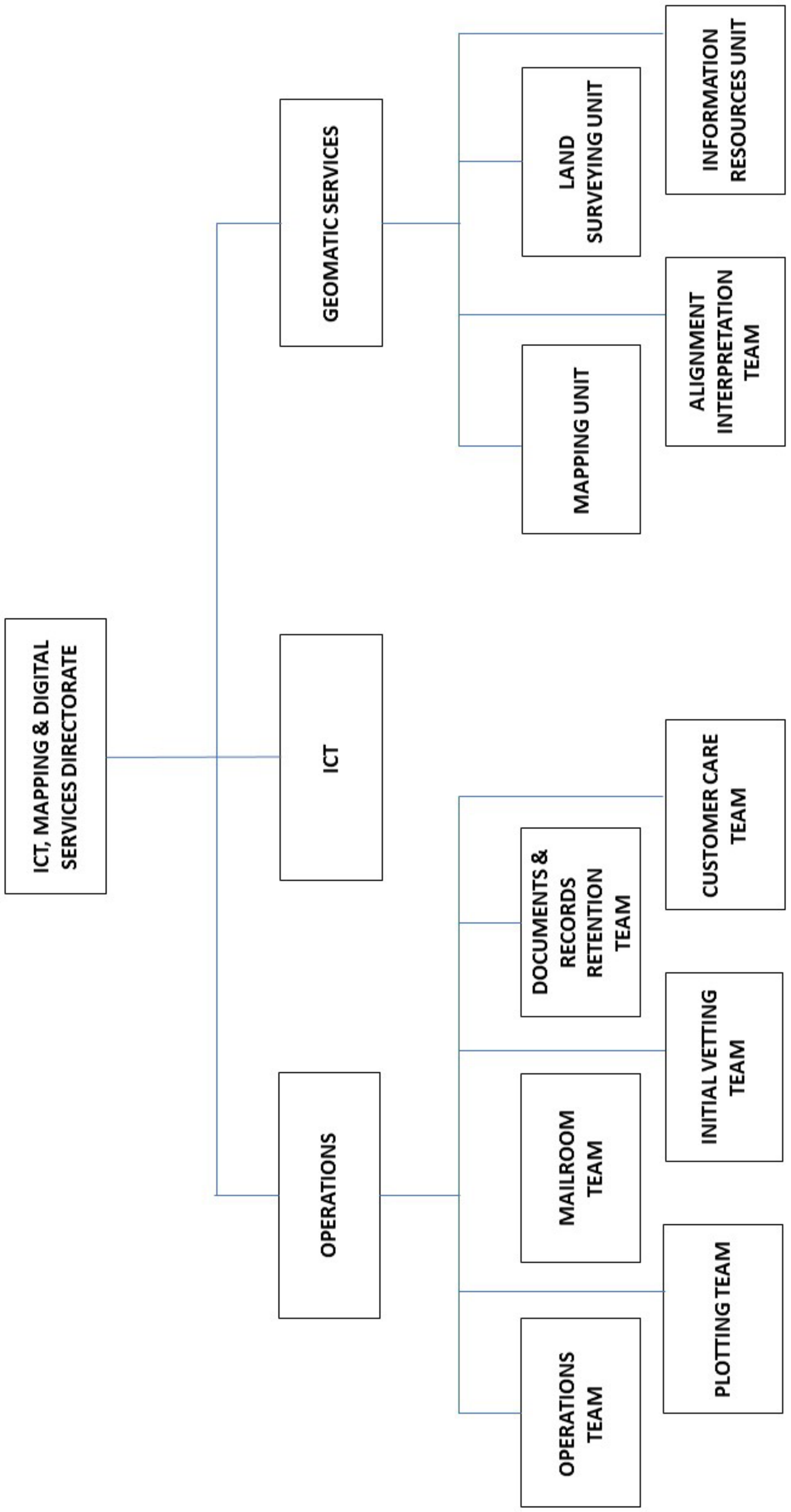
Planning Authority Organisational Charts *cont...*


COMPLIANCE & ENFORCEMENT DIRECTORATE
DIRECT ACTION
ENFORCEMENT ADMINISTRATION
ODZ & SECTORS UNIT
DEVELOPMENT ZONE, GOZO & COMPLIANCE CERTIFICATION UNIT

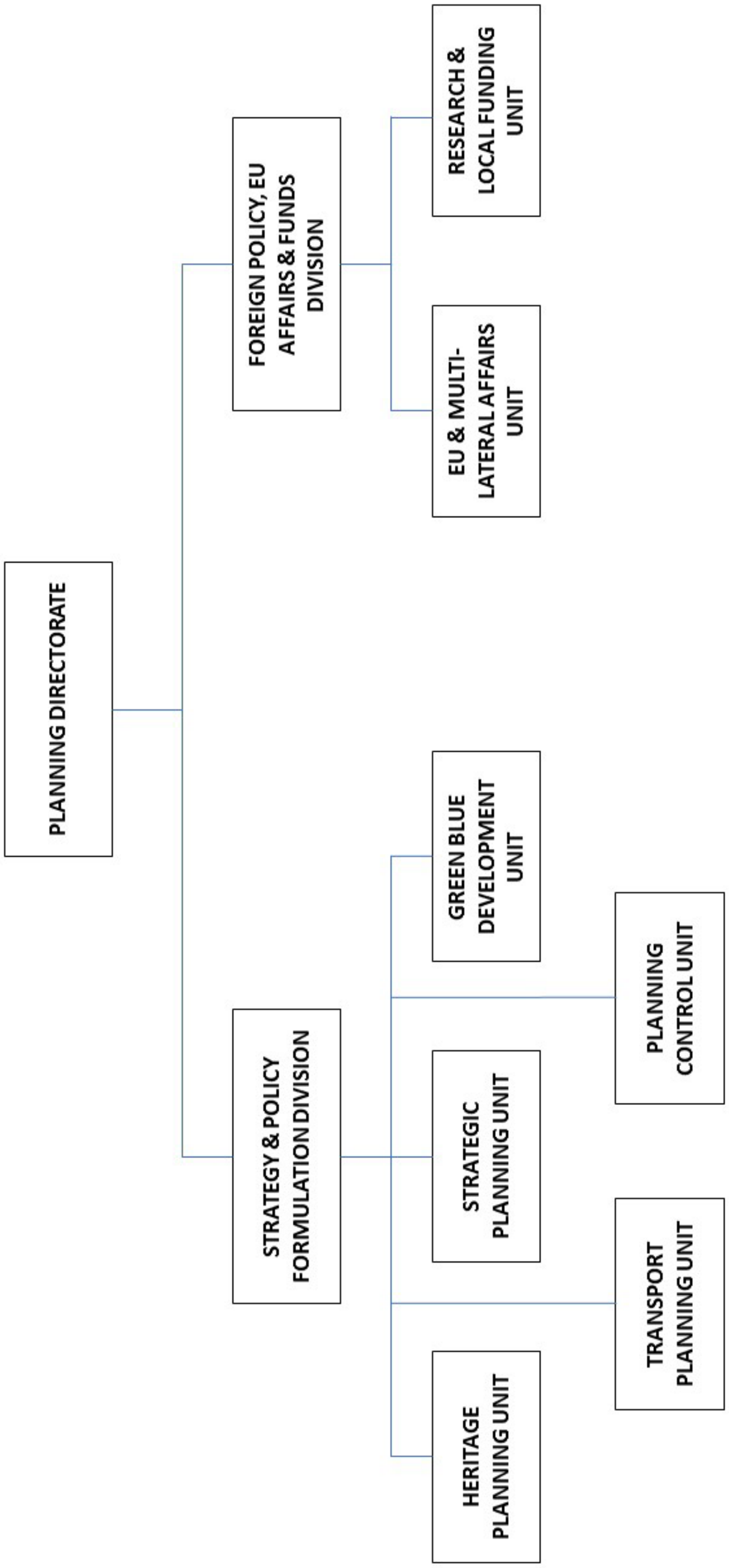
Planning Authority Organisational Charts *cont...*



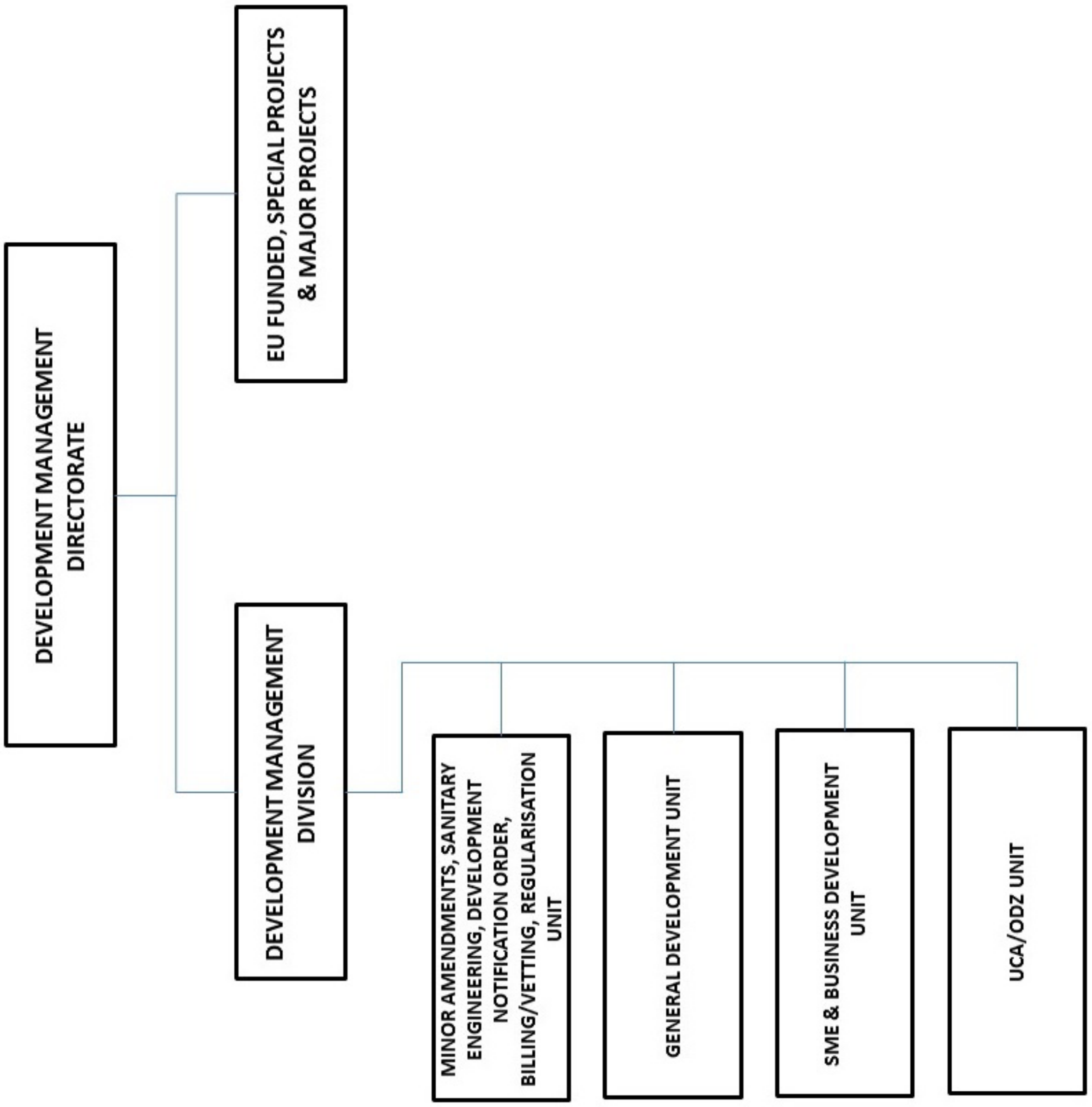
Planning Authority Organisational Charts *cont...*



Planning Authority Organisational Charts *cont...*


PLANNING DIRECTORATE
FOREIGN POLICY, EU AFFAIRS & FUNDS DIVISION
EU & MULTI-LATERAL AFFAIRS UNIT
RESEARCH & LOCAL FUNDING UNIT
STRATEGY & POLICY FORMULATION DIVISION
HERITAGE PLANNING UNIT
TRANSPORT PLANNING UNIT
STRATEGIC PLANNING UNIT
PLANNING CONTROL UNIT
GREEN BLUE DEVELOPMENT UNIT

Planning Authority Organisational Charts *cont...*


DEVELOPMENT MANAGEMENT DIRECTORATE
EU FUNDED, SPECIAL PROJECTS & MAJOR PROJECTS
DEVELOPMENT MANAGEMENT DIVISION
MINOR AMENDMENTS, SANITARY ENGINEERING, DEVELOPMENT NOTIFICATION ORDER, BILLING/VETTING, REGULARISATION UNIT
GENERAL DEVELOPMENT UNIT
SME & BUSINESS DEVELOPMENT UNIT
UCA/ODZ UNIT

2019-2020 (to date) Reports issued by NAO

NAO Work and Activities Report

April 2019	Annual Report and Financial Statements 2018 - Works and Activities

NAO Audit Reports

October 2019	Information Technology Audit: The Effective use of Tablets in State, Church and Independent Primary Schools
October 2019	Follow-up Reports by the National Audit Office 2019
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
May 2020	Annual Report and Financial Statements 2019
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.