NAO
National Audit Office
MALTA

Information Technology Audit

Inland Revenue Department

Table of Contents

Appendices

Figures

List of Abbreviations

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

ARS	Accounts Receivable System
AS	Anti Spyware
AV	Antivirus
BPR	Business Process Re-engineering
CdB	Common Database
CIO	Chief Information Officer
CLS	Computer Liaison Section
COBIT	Control Objectives for Information and related Technology
CPU	Central Processing Unit
CTD	Capital Transfer Duty
DDT1	Duty on Documents and Transfers
E-mail	Electronic Mail
ERFS	Electronic Request for Service
ETC	Employment and Training Corporation
FAQ	Frequently Asked Questions
FSS	Final Settlement System
FSSFBT	Final Settlement System Fringe Benefit Tax
ICT	Information and Communications Technology
ID	Identity
IMU	Information Management Unit
INI File	Initialisation File
IPS	Intrusion Protection System
IRD	Inland Revenue Department
IS	Information Systems
IT	Information Technology
LAN	Local Area Network
MAGNET	Malta Government Network
Mbps	Megabits per second
MFEI	Ministry of Finance, the Economy and Investment
MFSA	Malta Financial Services Authority
MITA	Malta Information Technology Agency

List of Abbreviations

MITC	Ministry for Infrastructure, Transport and Communications
MSM	Marval Service Management
MTPD	Maximum Tolerable Period of Disruption
NAO	National Audit Office
PAYE	Pay-As-You-Earn
PC	Personal Computer
PT	Provisional Tax
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SEP	Symantec Endpoint Protection
SSC	Social Security Contributions
TCU	Tax Compliance Unit
TPS	Taxpayer Services
VAT	Value Added Tax
WSUS	Windows Server Update Services

Chapter 1

Introduction

Chapter 1 – Introduction

The Inland Revenue Department (IRD) is responsible for the administration of the Income Tax and Duty on Documents and Transfers Acts and the enforcement of social security contributions (SSC) under the direction of the Ministry of Finance, the Economy and Investment (MFEI). The Department's objectives are to:

- ensure everyone duly complies with their tax obligations;
- provide improved services to support and reduce compliance costs on taxpayers and stakeholders;
- increase internal efficiency and reduce cost of tax collection;
- contribute to economic and social development; and
- develop its staff, processes and technology to make sure it remains a capable, responsive, results-oriented organisation.

The Department has an ongoing process of business process re-engineering (BPR) that complements the Department's objectives and Ministry's initiatives to simplify internal processes through the implementation of information systems (IS). The re-engineering includes:

- reviews of legislation, rules, processes and enhancements of back office IS;
- implementation of on line services for taxpayers, tax practitioners and third party data providers; and
- the acquisition of information from other Government Organisations to ensure full and timely compliance of all taxpayers whilst reducing the inconvenience on taxpayers to gather the same information.

This document is a report issued by the Information Technology (IT) Audit Section within the National Audit Office (NAO) covering the Inland Revenue IT Audit exercise as detailed in the Audit Section (Section 1.5). It documents the current state of IT operations at the IRD and provides an inventory of the technology and business processes associated with the Department as at report writing date.

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

1.1 Background

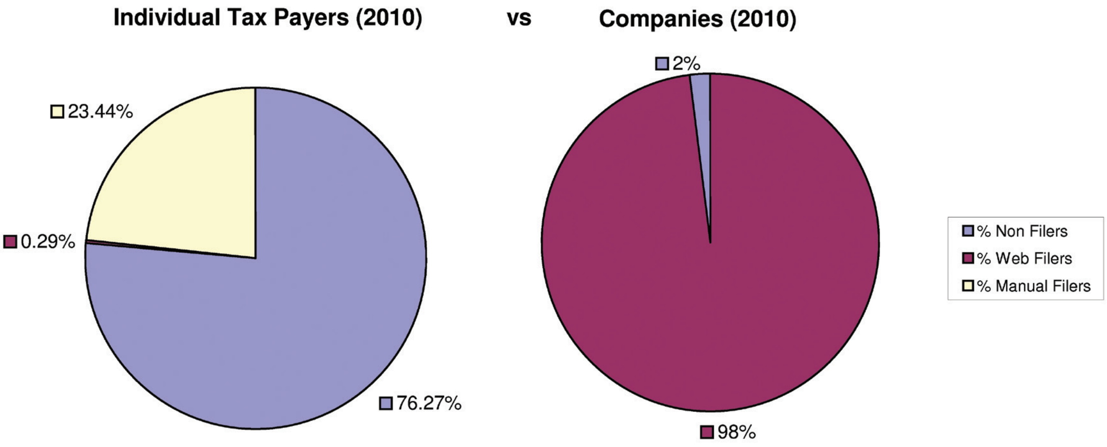
The IRD's main business process deals with the Income Tax Return cycle.

□ Between January and March, the Department initiates the information gathering processes from the various information sources including employers, data providers (private schools, care for the elderly etc.) and other Government Departments. This data is eventually analysed through a risk-assessment process to identify new registrations and distinguish non-filers from tax-return filers. Non-filers are those taxpayers whose income information is known by the Department through the various sources and hence are not legally obliged to file their income tax return to determine their tax liability.

□ During the same period, the Department informs companies to submit their annual tax return. Over 95% of Corporate Income Tax Returns are submitted on line by tax practitioners. (Source: IRD)

□ In the months of May and June, the Department issues the tax return / non-filer statements to all those individuals who were active in the previous calendar year. During this period, the activity at the Department's call centre and taxpayer services sections increases substantially.

Figure 1 - Method used by Companies and Individual Taxpayers to file tax returns (2010)



Source: IRD

- □ Submitted tax returns are then captured during the summer months and eventually statements are sent to taxpayers towards the end of the year.

During the year, there are various other routine business procedures including:

- □ Provisional Tax (PT) Payments / Class 2 SSC[1]
- □ Enforcement and Collection
- □ Tax Audits, Investigations and Objections
- □ Collection of Final Settlement Tax and Class 1 SSC[2]

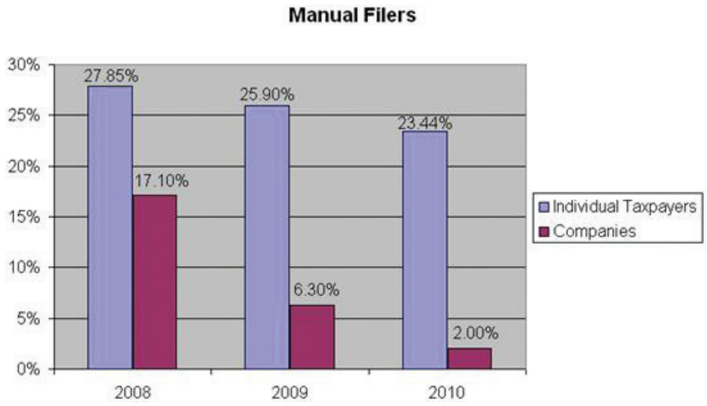
The IRD's Website provides the facility of filing tax return online. This facility is provided to both the individual taxpayers and the companies.

As depicted in Figure 1, whilst the majority of the companies utilise these online facilities to file their tax returns, the individual taxpayers still prefer the manual option.

It is however encouraging to note that the number of manual filers has in the past three years decreased every year. This is depicted in Figure 2.

Apart from the facility of filing tax returns online, the IRD has developed a facility through which employers could submit FS7 Forms and FS3 forms of their employees online. Figure 3 overleaf details the methods used by employers for submitting their FS3 forms during basis years 2008, 2009 and 2010.

Figure 2 - Manual Filers during the last 3 years

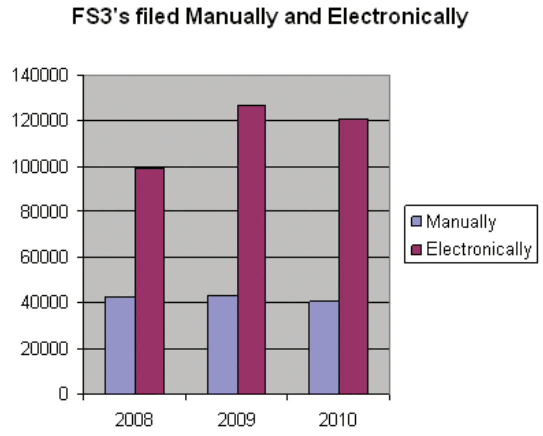


Source: IRD

[1] "Class Two contribution" means a contribution which an insured person pays either as a self-employed person, or as a self-occupied person

[2] "Class One contribution" means a contribution that an insured person pays as an employed person (available from http://www.mpo.gov.mt/downloads/Manual-SocialSecurityContributions-Benefits.pdf)

Figure 3 – FS3's filed manually and electronically during 2008, 2009 and 2010



Source: IRD

1.2 Organisation Structure

The IRD is presently divided into seven main directorates:

- □ Administration & Enforcement
- □ Operations
- □ Tax Audits
- □ Technical
- □ International Taxation Unit
- □ Tax Compliance Unit (TCU)
- □ Capital Transfer Duty (CTD)

The Department's main premises are located in Floriana and consist of six separate adjacent blocks. As at September 2011, the IRD has a staff compliment of 239 full-time employees of which 174 are posted at the Inland Revenue Blocks in Floriana. The Department has another office in Victoria Gozo with a staff compliment of 17. Moreover, the Department's International Taxation Unit is located at the Malta Financial Services Authority (MFSA) building in Attard and has a staff compliment of four whilst the CTD is located in Merchant Street, Valletta with a staff compliment of 44 employees.

In line with Government's family friendly measures policy, IRD has a number of employees working on teleworking basis. The number of employees availing themselves of teleworking opportunities is 27 amounting to about 11% of IRD's total workforce.

The organisation charts in Appendix A depict how the IRD is set up.

1.3 Laws/Legislation

The Department carries out its functions under the following legislations:

- □ The Income Tax Act (Chapter 123)
- □ The Income Tax Management Act (Chapter 372)
- □ Duty on Documents and Transfers Act (Chapter 364)
- □ The Death and Donation Duty Act (Chapter 239)
- □ Goldsmiths and Silversmiths Ordinance (Chapter 46)
- □ Monte di Pieta' Act (Chapter 269)
- □ Immovable Property (Acquisition of Immovable Property by non-Residents) Act (Chapter 246)

The tax determination and calculation is also affected by other peripheral legislation such as the Business Promotion Act, the Merchant Shipping Act and the Stock Exchange Act.

1.4 IT at the Department of Inland Revenue

Considering the extensive amount of data managed by the department, information is undoubtedly one of the most important assets at IRD. Thus the way this information is managed and processed is of fundamental importance particularly in view of its extremely sensitive and confidential nature. Hence, the need to ensure maximum security and reliability cannot be over-emphasised.

The IT Systems used at the Department of Inland Revenue are:

- Accounts Receivable System (ARS) – The ARS is the department's main accounting system. All taxpayer accounts are maintained in this system. Transactions are posted into ARS in batches through the process application. Payments received are posted in ARS through the in-built receipting modules.

- Return Capture – This system is used to capture tax returns and adjustment forms and view tax statements and information related to taxpayer information.

- Acknowledgement – The Acknowledgment system is used to acknowledge income tax return documents including tax returns, adjustments forms and other similar documents.

- Process Software Application - This software application is used exclusively by staff at the Computer Section. This software application is the module that triggers the batch processing of the Inland Revenue. Processing includes generation and printing of returns, tax statements, PT and SSC claims and refunds.

- Web Directory – This system is used to process Inland Revenue Services online forms. The main function is to register and maintain web users and link companies with tax practitioners as authorised through Inland Revenue Web form 2. Along with the processing of IRWEB02's, which are related to tax practitioners, this software application is also used to assign access to employers in relation with Final Settlement System (FSS) online services (IRWEB06's), add users to tax practitioners (through IRWEB03) and register new tax practitioners (IRWEB01). This software application also provides functionality to grant access rights to data providers.

- Web Process - The Web Process synchronises the web and live environments. This includes the generation and loading of electronic company tax returns onto the web environment and transfer of documents and returns submitted by web users. Internet banking and credit card payments are also loaded onto the live environment through this application.

- Inland Revenue online services - This is a suite of web services for registered Tax Practitioners (primarily consisting of company auditors), Employers and Individuals. Amongst others, tax practitioners may submit Income tax returns and Financial Statements on behalf of companies. Employers may submit FS5s, FS7s and FS3s online whilst individuals may submit their personal tax return.

- Power Panel - This application consists of two main modules, namely the access rights management to IRD applications and the generation of penalty reduction scheme notices.

- IT1 - IT1 is the old assessment system (up to Year of Assessment 1998) thereafter substituted by the Return Capture system. Information submitted through returns used to be captured from this system in order to raise assessments.

- FSSFBT/FS7 Document Management - These two separate modules are used to generate requests for submission of FSS documents to employers, acknowledge and manage the documents received, process the FS3s and FS7s received in paper form or online.

- Taxpayer Services (TPS) - The TPS supports three inter-related processes being:

  - Document Management – All incoming correspondence is indexed, scanned and viewed through TPS.

  - Taxpayer enquiries, personal encounters (at taxpayer service) and telephone calls are logged by respective sections in TPS.

  - Queue management – Incoming correspondence and taxpayer enquiries are linked with specific processes – such as address change/objections etc to create tasks. Tasks are then directed in the queue of the respective officer in charge of that specific task. Once the task is executed, the officer in charge closes the task accordingly.

- Person/Company/BOP/Employer Index - These applications hold the registration details for each of the four main taxpayer types. New taxpayers are created and maintained from these applications.

- CTD Software Applications – These are a set of modules used by the CTD in Valletta and Gozo. Primarily these are used to capture *Inter-vivos* and *Causa-Mortis* transfers of property and shares in private companies. Separate modules exist for the receipting of Duty on Documents payments, capturing of architects reports and issuing of additional assessments following architect's valuation of immovable property.

- Call Logging System - The call-logging system was based on a workflow engine (product). This was subsequently replaced by the TPS in view of substantial increase in licence costs and due to the fact that the re-engineering done did not utilise in full the facilities of the workflow engine.

- On Line History - This is an electronic archive of past tax data (Swatar period). Any information on assessments, Pay-As-You-Earn (PAYE) and payments which were done prior to the implementation of the electronic system has been loaded into this application. Such tool results useful to any IRD user which may need to perform a detailed analysis on a particular taxpayer on years where the manual system was still in place.

- Audit Desktop - This application is used by the Tax Audits Section to keep track of ongoing tax audits.

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

- Return Capture
- Acknowledgement
- Process Software Application
- FSSFBT/FS7 Document Management
- Audit Desktop

1.5 Audit Scope and Objectives

The scope of this engagement was to analyse the IT and the IS used by the IRD, identify any potential risks and make recommendations to mitigate those risks.

The IT Audit carried out consisted of two stages:

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

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

Therefore the objectives of this report were to:

- document all the information collected during the numerous interviews held with various officials;
- summarise the documentation collected and elicit the area/s of concern;
- determine whether the Inland Revenue's IT systems operate effectively, efficiently and economically;
- record the findings and identified related risks; and
- list the NAO's recommendations.

1.6 Audit Methodology

In order to attain the above objectives a number of interviews were held with various officials at the IRD. Interviews were also held with officials at the Malta Information Technology Agency (MITA).

Reference was also made to the Control Objectives for Information and related Technology (CoBit) 4.1 set of best practices. CoBit 4.1 specifies two types of controls, namely General and Application. The controls that were considered during this audit are listed in Appendix B.

1.7 Structure of the Report

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

□ Chapter 2 deals with the IT management perspective.

□ Chapter 3 reviews a selection of Inland Revenue suite of software application in greater detail.

□ Chapter 4 evaluates the Protection of Information Assets.

□ Chapter 5 assesses the Risk Management, Business Continuity and Disaster Recovery procedures.

□ Chapter 6 lists the Management comments.

1.8 Acknowledgements

NAO would like to express its thanks and gratitude to all the staff within the IRD, particularly the Commissioner and MITA who were involved in this audit, for their time, patience and assistance.

Chapter 2

IT Management

Chapter 2 – IT Management

2.1 IT Unit

The Inland Revenue has an IT unit which is referred to as the Computer Liaison Section (CLS). The functions of this section are to:

- liaise with suppliers on IT projects and software enhancements;
- carry out the user acceptance testing of software applications and of enhancements to software applications;
- provide all the IT assistance and support required internally by other sections within the IRD;
- run a helpdesk for external web users such as Tax Practitioners and employers and third party providers; and
- execute end-of-day scripts related to batch processing and bulk printing.

The CLS reports to the Director of Administration & Enforcement of the IRD and communicates with the Ministry's Information Management Unit on a regular basis.

The CLS section is made up of seven officers comprising of a manager, two technical persons and four support staff. The officer heading this section was appointed in April 2009.

During the course of this audit, the NAO noted that a number of functions being carried out by this section are dependant on a few key members of staff. The process of executing the 'end-of-day' routines, carrying out the related batch processing and dealing with the bulk printing is the responsibility of one staff member. This may lead to an unsustainable workload and a high or total dependency on the present staff. Such a sensitive process and other similar processes should not be dependant on the availability of a particular person and, ideally, other staff need to be trained in these areas. IRD clarified that although one person is currently handling certain functions, other IT employees have the necessary skills to step in when required.

Thus, the National Audit Office welcomes the fact that the Inland Revenue Department has issued a call for applications so as to increase the resources in this section and therefore mitigate the above mentioned risk. IRD subsequently informed NAO that the selection process was completed at the end of May 2011.

2.2 IT Strategy

Although the IRD has a documented Programme Plan it does not have a formally documented IT strategy. Indeed the Commissioner of Inland Revenue has conducted a number of meetings with both the Ministry's Information Management Unit and the CLS in order to formulate an IT strategy.

The Department's IT strategy is targeted towards:

- reducing, as far as possible, compliance burdens on taxpayers and information providers;
- maximising tax compliance (income declarations, payments and document submission);
- improving the efficiency of internal processes to reduce cost of collection;
- improving the services provided to taxpayers, employers and tax practitioners;
- providing adequate and accurate reporting facilities; and
- ensuring that applications have the necessary controls to prevent unauthorised access/changes to critical and confidential information.

The IRD is specifically aiming at reviewing its internal processes on an annual basis and implement the required IT improvements to support the revised processes. These changes in internal processes are mandated by legislative and policy changes but also include internal BPR. The e-business web site is continuously enhanced to provide better services to taxpayers, tax practitioners and employers based on their feedback. More interaction with other Government Departments is also planned improving upon the exchange of information and reduce requests for information from taxpayers when this has already been submitted to one Government Department.

The IRD's planned IT/IS projects include:

- Implementation of a facility to submit the following documents over the web:
  - Adjustment forms for companies
  - Shareholder Registration form
  - Refund Claim
  - Other basic forms such as address change etc
- Integrated Employment and Training Corporation (ETC) engagement form and FS4 (Joint project with ETC);
- Facility for notaries to submit the Duty on Documents and Transfers (DDT1) forms and related payments over the web;
- Implementation of inter-departmental measures to address non-compliance in return submission of Income Tax Returns and Value Added Tax (VAT) Returns;
- Enhancement to Internet Banking services;
- Enhancement of Outgoing/Incoming mail management facilities;
- Automation of various existing manual processes within the computer section;
- Various enhancements to enforcement processes and related reporting facilities;
- Enhancements to applications to improve internal controls; and
- Improved reporting including that related to Risk Analysis to Revenue.

Whilst recognising the fact that, as informed by the respective Ministry's Chief Information Officer (CIO), IRD and MITA met to discuss the Taxation programme for the coming years, NAO suggests that the IRD drafts a formally documented IT strategy. The IT strategy should focus on creating and measuring business value from the investment carried out in IT. It is recommended that this strategy should formally document:

- the above mentioned IT/IS projects and improvements;
- cover the developments being planned for the next three to five years; and
- reference to the Logical and Physical architecture of the Inland Revenue's IT systems.

2.3 IT Budget

The IRD's IT budgeting cycle for the subsequent year, starts in June/July with the submission of the estimates of the planned IT/IS projects and improvements requested by the Department. This submission is done through a joint effort involving the department's senior management, the related Project Manager within MITA and the MFEI CIO. These estimates are submitted to and reviewed by the MITA Business Planning Team and prioritised by the MITA Board depending on:

□ National priorities.

□ Strength of Business Case.

□ Contractual commitments already in place.

The above-mentioned estimates are based on costings from previous years for the development and implementation of:

- software enhancements related to the implementation of Budget Initiatives; and
- IT/IS enhancements resulting from the yearly Tax Return cycle. Typically these include enhancements to the various systems to improve:
  - taxpayer services
  - internal operational efficiency
  - 'Inland Revenue Services On-Line' (the suite of e-business applications of the Department).

Subsequently the IT/IS requirements are revised in line with the actual budget allocations and requirements. A programme of works is drawn up to meet the above mentioned revised IT/IS requirements which may only be changed through the agreed change management process during the course of the implementation.

As part of this audit the NAO sought to identify the percentage of the IT budget going towards new IT investment and the percentage of the IT budget going towards IT support. In 2010, 17% of the budget was dedicated to support and 83% was allocated towards new IT investment.

The NAO recommends that the IRD together with the Ministry's CIO carries out an exercise to ensure that all its IT and IS operational costs are clearly identified in order to carry out related cost-benefit analysis. This analysis would constitute one of the critical factors in the drawing up business cases to be forwarded to the Ministry, for planned IT/IS procurement at IRD.

2.4 Project Life Cycle

During this audit, the NAO has reviewed the project life cycle adopted by IRD in terms of procuring new

hardware, procuring new software and the development of enhancements on existing software.

2.4.1 *Hardware project life cycle*

As detailed in 2.6 below, the IRD procures most of its IT equipment through the personal computer (PC) leasing scheme. Other IT equipment which may be needed, but is not covered under such agreement, is procured by the CLS. The procurement process adopted by the CLS includes the following steps:

- A requisition is made to the CLS.
- CLS verifies the need, estimates the costs involved and seeks to obtain the necessary approvals.
- Once the necessary approvals are obtained, CLS procures the required hardware.

2.4.2 *Software project life cycle*

Since all the Software Applications owned by the IRD are managed and maintained by MITA, the IRD relies on MITA's software project life cycle.

The NAO has thus reviewed the project life cycle followed in terms of procuring new software and implementing enhancements on existing software. MITA's software development procedure establishes seven major phases with the development life cycle as defined below:

□ Initiation and Planning

□ Requirements Definition

□ Design

□ Development

□ Integration and Testing

□ Implementation

□ Maintenance and Enhancement

So as to ensure that the project life cycle implemented was sound, the NAO examined the project life cycle adopted in the scenarios detailed below.

In 1999 the IRD implemented the Self-Assessment regime and as a result instructed MITA to implement a number of software applications to support this reform. These applications underwent changes on an annual basis to implement major programmes or changes announced in the Budget of the respective year or in other Government Initiatives such as the National Reform Programme. These software applications were also enhanced to reflect ongoing BPR done by the IRD to:

- improve controls;
- reduce operational costs;
- increase compliance; and
- improve taxpayer services.

Furthermore, software applications are also enhanced on an ongoing basis to keep them in-line with the current technical platform upgrades and best practice. These upgrades include:

- development environment tools;
- database management systems; and
- server and client operating systems.

Examples of best practice enhancements include exposure of business functions as web services so that these can

be consumed by various applications (e.g. the automatic registration of companies through the consumption of a web service implemented by the Registrar of Companies). Maintenance and Support tasks are also carried out so as to correct software bugs, implement minor changes to business rules (such as additional validations) and provide operational support.

In all these scenarios, the process will initially identify the changes and enhancements required. These enhancements are then scheduled for implementation. In general, the prioritisations for scheduling, is as follows:

- Level One: Immediate if bug fixing is required especially if operational issues arise. Similarly, if technical platform updates are required to improve security or performance, these are given immediate priority.

- Level Two: Enhancements to implement budget and other initiatives related to the Tax Return cycle follow as these will be related to tax submission dates.

- Level Three: Enhancements that will improve operational efficiency and implement other initiatives will then be implemented. Within the priorities, work can be allocated if changes are not extensive or do not carry major impact to testing and implementations.

Generally, given the complexity and integration of the Taxation Systems together with the volumes of information contained in these systems, the project team collaborates with Department officials to develop business models that will reflect the effect of the new enhancements. This aids the development process, and subsequent testing and implementation. Usually enhancements are required on existing modules but sometimes new modules may have to be delivered together with enhancements to existing ones (e.g. the scheme to collect Income Tax Arrears required both new modules to generate letters and enhancements to the Return Capture and other modules).

All new software modules and enhancements procured would go through a cycle of rigorous testing that would also involve user acceptance testing prior to implementation.

The IRD has no plans to decommission any of its software applications in the foreseeable future. In the past, applications no longer required within the main operational cycle, were still maintained and supported. Due to the historical nature of tax transactions these applications would still need to be accessed and used over a number of years until they can be decommissioned.

In cases where applications are replaced, these will be archived by MITA's project team, within the configuration system such that they will not be released again. No further maintenance work is done on such applications that have been replaced.

The NAO feels that although MITA adopts a sound project life cycle, that ensures appropriate project management in the development of new software modules as well as in deploying enhancements to existing software, it would be ideal if IRD would be able to take an increasingly participative role at different points in the project life cycle i.e. in the design, planning and scheduling of the project.

2.5 Third Party Suppliers

The IRD receives all the required IT support from MITA.

In line with the Government's policy on consolidation and centralisation of core information and communications technology (ICT) services announced in OPM Circular 29/2005, MITA entered into a Core Services Contract with Government for provision of 'core ICT services' to Ministries, Departments and a number of public sector entities.

The owner of this contract on behalf of Government is the Ministry for Infrastructure, Transport and Communications (MITC).

NAO notes that this contract includes a service level agreement that stipulates the service levels applicable to each specific service, namely:

- □ E-mail
- □ Internet
- □ Network Workstation Support
- □ Local Area Network (LAN) support
- □ Calls reported to MITA's Service Call centre
- □ Application Maintenance and Support.

This agreement classifies any incident or task relating to the above areas, according to a priority level which may be Critical, High or Normal. Each of these priority levels is defined in this agreement.

The IRD has stated that these service levels have up to now proved to be adequate to the daily needs of the Department.

2.6 PC Leasing Scheme

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

During 2009/2010, the IRD replaced all desktop computers and laptops through the PC leasing scheme. Since the desktop computers and laptops are now relatively new, this scheme has reduced much of the maintenance burden that previously fell on IRD's CLS. Furthermore, requests of maintenance and repairs are now being handled by MITA through the CLS and serviced by the third party suppliers who were awarded the tender. Given this situation, computers may need to be taken out of the Department's premises to the third party's workshop. Due to the fact that all hardware is relatively new, the need to have hardware serviced outside IRD premises has never occurred until now. Yet this still presents a major risk to the Department since the hard disks of IRD computers are likely to contain highly sensitive data about both individual taxpayers and companies. The NAO has however been informed that, in order to address such risk, the Department is liaising with the Information Management Unit (IMU) to design and implement a policy and procedure to cater for instances were a PC needs to be taken out of the Department's premises. This policy is intended to protect and prevent information located on hard disks in the event a PC needs to be taken out of the Department's premises.

Secondly, the computers are now assigned to employees and therefore when an employee is transferred to another department he/she is expected to transfer his/her computer. As explained above, this practice may expose IRD to risks similar to the ones detailed in the case above, in which pc's/laptops possibly containing sensitive IRD data are taken out of the Department's premises. The NAO recommends that the IRD takes all the necessary steps to ensure that any employees who left the IRD (including employees transferred to other Ministries/Departments) would not be able to access any IRD data through their desktop computers and/or laptops exactly before to their transfer to other Departments. NAO has noted that IRD has issued a memo in 2006 instructing staff not to save any data on their hard disks but utilise their personal folder or their section's folder on the server. NAO recommends that IRD issues a reminder of such memo.

2.7 Network Infrastructure

The IRD is connected to the Government Network referred to as MAGNET. Connection is being made through a dual fibre link. MITA is responsible for maintaining IRD's network infrastructure.

During the course of this audit, the NAO requested a network diagram and reviewed the network setup and its availability.

The NAO recommends that the IRD should take steps to ensure that:

- all network switches are connected to a UPS whose battery is tested on a regular basis; and
- all current network switches are monitored for Central Processing Unit (CPU) utilisation and upgrade where old switches are still in operation.

NAO has observed that IRD receives specific email notifications from MITA/IMU when the particular drive or share reaches 85% of the allocated space.

NAO noted that there were two types of notifications:

- folder quota warnings over Project or Application folders; and
- folder quota warnings over home-folders.

Furthermore NAO noted that when users approach CLS following a receipt of warning over their home folder, CLS asks users to review the contents of their home folder and remove any personal (not work-related) content. Users are also urged to transfer any work-related data into a project folder rather than keeping it in their personal folder.

Although, as detailed in the preceding paragraph IRD receives notifications when home folders reach 85% of the allocated space, the NAO suggests that IRD takes a proactive approach and requests a monthly report from its service provider, detailing the home folder quota usage of its employees. This report would help IRD detect inappropriate use of the home folders thus occupying capacity which could be put to better use by the Department. IRD may also consider implementing file screening so as to prevent users from storing certain files on their home folders. Furthermore IRD can even configure the file servers to notify the administrators by E-mail when users try to save files that are blocked by file screens.

2.8 IT Inventories

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

The IRD has an IT inventory which is updated on a regular basis and includes all the relevant details such as the person making use of the particular IT asset, the section in which it is located, its inventory and serial numbers and its asset category. The NAO was informed that this inventory was currently being reviewed to ensure its accuracy and completeness.

However, the NAO has observed that the IT inventory supplied by the IRD included only desktop computers, laptops, printers and print servers. Such inventory should be updated so as to include all the devices that the IRD may have such as scanners, projectors, ups', external hard drives, external DVD writers, digital voice recorders, projectors and all monitors. The NAO has been informed that the above information is being collated by the Ministry's CIO and it is therefore being recommended that IRD requests the required information from the Ministry's CIO on a regular basis.

Furthermore, NAO observed that in 2009/2010 the IMU has produced an IT Software inventory detailing IRD's Client/Server Applications. NAO recommends that this inventory is updated so as to include all software including the office automation tools used by IRD. This is very important so as to be able to account for all software licenses being paid, as well as to make sure that all licenses are being made use of.

Chapter 3

IT Applications

Chapter 3 – IT Applications

During the course of this audit the NAO has observed that Inland Revenue's IT applications are all part of the Department's workflow. Furthermore, business processes and related supporting software applications are continuously under review to improve work flows and increase efficiency.

The NAO noted that during the implementation of the yearly Income Tax Return cycle, the Department reviews both internal business processes and taxpayer facing processes to increase efficiency and improve taxpayer facing procedures.

The Department has also affected a number of BPR exercises over the past 10 to 15 years within the scope of major Tax Reforms, Central Government initiatives and other Ministry or Department initiatives. During such initiatives software applications, business processes and, if necessary, legislation are reviewed and updated accordingly. The following are the most prominent BPR exercises carried out:

- In 1997-1998 the self assessment system was implemented and as a consequence most of the Departments' processes were re-engineered. Where information was available about a Taxpayer, the Taxpayer was requested to submit a simple Tax Declaration rather than a full income Tax Return. The Tax Return was also simplified as a document to facilitate completion by Taxpayer. Automated penalties and additional taxes were also implemented. Overall efficiency increased substantially since assessments were now being printed within the same year. All IRD systems were changed following this BPR which resulted in a significant increase in revenue.

- During the same years, the FSS system was implemented to replace the former PAYE system. With the implementation of the FSS, the tax due by employed taxpayers started being calculated and deducted at source, thus reducing the number of balances and refunds due from fluctuating employment income at year end. Taxpayers were automatically registered from employers, ETC and Common Database (CdB) and hence did not need to call at the Department to register or to have their PAYE tax rate calculated. Furthermore, the revenue lag from PAYE was eliminated as Tax was being collected in time when it arose; hence reducing the occurrence of balances and or refund being paid years later.

- In 2002, the Department launched the E-return for companies. Within a few years, over 95% of company tax returns were being submitted through the web thus eliminating the need to capture vast amounts of data. Through this change, company declarations (including Financial Statements) started being received in a structured way (without any user intervention or interpretation), thus improving the Department's reporting capabilities.

- In 2007, the Department launched the Non-filer system instead of the former so-called 'simple tax declaration'. This was possible as online systems were implemented for employers; hence the information could be processed within a relatively shorter timeframe. Furthermore any tax incentives for various social or economic measures were implemented using a mechanism that collects information from a provider. Hence, where the information about a taxpayer is known by the Department, the taxpayer is not required to send any documentation and will be issued a Tax Statement. The Non-filer initiative affected 70% of all individual taxpayers. As a result of this BPR exercise, these taxpayers, mostly employees, pensioners and students were not required to fill any income tax declarations. This initiative saved the Department the effort usually required to process about 155,000 of declarations annually. This measure also helped to increase the compliance rate.

The NAO was informed that as in previous years the Department will be reviewing its procedures again during the 2011 Income Tax Return cycle, implementing various enhancements including:

- new web facilities for companies involved in Financial Services;
- improve document management processes for structured documents; and
- various improvements in the department's enforcement and reporting systems.

For the purpose of this audit and as mentioned in Chapter 1, NAO has evaluated the five major applications listed below:

□ Return Capture

□ Acknowledgement

□ Process Application

□ FSSFBT/FS7 Document Management

□ Audit Desktop

MITA has a dedicated team composed of nine persons, including a Project Manager, who are responsible for the ongoing development and support which is needed by the IRD in connection with its software applicatios. Given the criticality of certain IRD software applications, NAO recommends that MITA and IRD all steps necessary to avoid any dependency on one particular person to provide support on the above software applications.

The NAO has also noted that user manuals were only available for two applications and in both cases these manuals were dated 1999. The NAO recommends that IRD requests MITA to supply the required user and programming manuals as soon as possible.

In the case of the five applications which have been audited, the administrative role is shared between MITA and IRD's CLS. Whenever a new user is to be created the CLS submits an Electronic Request for Service (ERFS) to MITA. The latter then adds this new user through a centralised application. The CLS would then assign the necessary security rights pertaining to that particular user.

As detailed in the paragraph above, access to all five listed applications is through a centralised application and therefore each user accessing more than one application uses the same username and password for all modules. The NAO noted that the operating system has in built algorithm/s that ensure that the password has adequate length and mix of syntax characters that make it complex. Furthermore, another feature of this algorithm is that it prevents use of dictionary and keyboard patterns from being used as passwords. The NAO also noted that the IRD and MITA has implemented a rigorous password management procedure whereby passwords expire after a set period and once a password is changed it cannot be reset for a predetermined amount of time.

When the user requests a password reset through MITA's Service Call Centre, the password can be changed upon first login. Furthermore, a password cannot be used again until a pre-determined number of password changes. The application is also blocked if a user attempts more than three unsuccessful tries at inputting the password. Users who forget their passwords are required to E-mail MITA's call centre requesting a password reset. The new password is then communicated directly to the user.

Security permissions are immediately revoked if an employee resigns, is transferred or is away on prolonged leave. This is done by the CLS upon notification from the HR Department within IRD. The NAO recommends that apart from revoking the security rights assigned to these employees, IRD clears the initialisation (INI) file so that these employees would not have the applications to which access was removed, appearing in their launcher.

Due to the nature of transactions, the Inland Revenue's software applications do not allow users to delete transactions and a record is kept in the audit tables of the other data which can be deleted. To quote just one example, whilst a receipt transaction cannot be deleted, a locality may be deleted from the list of localities; however, this deletion is still recorded in a deleted localities table. The Inland Revenue applications are thus equipped with complete audit trails that record all user actions including the username, date and time when each action was performed.

The NAO noted that the MITA project team has read only access to IRD's applications and write access is only given by exception and according to agreed change management procedure. This access was said to be required for support and debugging purposes.

The Department should ensure that every effort is undertaken to eliminate the risk that data integrity and confidentiality are compromised in any manner even in view of data protection considerations.

All the IRD's IT software applications are hosted on servers residing at MITA whose staff is also responsible for regular system maintenance and for ensuring that daily, weekly and monthly backups are taken. Such backups are also stored in safe repositories at an offsite location. The NAO was

also informed that these backups are periodically tested on a simulation environment. The last restore attempts were made in September 2010 and in May 2011, loading the data of a few days before. These tests were successful.

NAO was also informed that MITA processes all incidents, application updates, changes in the database schema through the MARVAL Service Management (MSM) system and therefore all changes are logged and recorded.

During the course of this audit, NAO also enquired about the manner in which data is received from third parties and the level of quality of this data and was informed that currently there are some data issues. The NAO recommends that IRD takes the necessary measures so as the web portal services are made use of by a larger number of data providers giving them the facility to upload their data online. This facility would allow data to be verified automatically and if need be corrected by the data provider there and then. Encouraging data providers to use such a facility would reduce the time taken by IRD staff to clean the data received prior to uploading it in the IRD software applications.

The NAO also enquired about any issues that may be present in the applications which were not being audited. NAO suggests that IRD reviews the ARS in terms of its level of user friendliness, its graphical user interface and the manner in which naming conventions are coded in the system making it difficult for new users to learn what these codes stand for. Any enhancements resulting from this review should be assessed by a cost benefit analysis.

3.1 Return Capture

The Return Capture System is used to capture the IRD's tax returns and adjustment forms. Furthermore the Return Capture System has the facility to display information regarding individual taxpayers and companies and view their corresponding tax statements.

This application was developed by MITA and deployed at the IRD in 1999 as one of the IT applications developed in order to support the self-assessment and Year by Year Accounting regime that came into effect as from Year of Assessment 1999.

During the course of this audit the NAO observed that this system has various levels of security rights which are assigned to according to their specific role. Read only facilities are available and these may also be restricted to particular screens. Furthermore, records of certain taxpayers with a mismatched undeclared income are only accessible by the Head of Section.

The NAO noted that during the time when a tax return document is awaiting to be processed , any subsequent document submitted by the taxpayer may not be captured until the first document is processed. This impacts negatively the turnaround of the process. NAO suggests that this process is investigated further so as to find a way where adjustment forms can be captured immediately.

The NAO observed that IRD requested a number of fixes concerning this application from MITA. Although all these fixes, with the exception of one, are classified as having a low or medium priority, some are dating back to November 2010. One particular fix reported in February 2011 was classified as of a high priority. After further investigation NAO noted that although this fix was not halting any of the Department's operations, since a workaround was devised, this workaround was proving to be time consuming impacting overall performance.

Furthermore, a number of enhancements were also reported to MITA and whilst the absolute majority of these are classified as having a low or medium priority these date back to December 2010.

NAO also noted that the Department is not given a target completion date when a bug or an enhancement is reported. NAO, thus suggests, that the Department and MITA agree upon target completion dates and if necessary IRD is to start discussions with MITA so as to see whether extra resources can be allocated on the project so as to reduce the present time-lags.

During the course of this audit, NAO observed that the CLS is requested to issue comprehensive reports encompassing a wide range of selection criteria providing management with the necessary tools to assist MFEI with the normal day to day information requirements. Since this is resulting in a lack of empowerment to the user, NAO suggests that such reports are implemented into the Return Capture System so as the user would be able to issue such reports directly without having to request the CLS to generate such reports and thus saving CLS a considerable amount of time.

Furthermore, NAO suggests that the present manual reports being issued out by each section head relating to staff performance, would be incorporated in a report that is generated by the system. This will increase timeliness, empower management and possibly help management in taking an earlier corrective action when this is needed.

3.2 Acknowledgement

The IRD records all income tax return documents in the acknowledgement system which is then used to acknowledge all the inputted documents including tax returns, adjustments forms and other similar documents. This system is integrated with a bar-code reader and tax returns and correction forms (issued by the IRD System) are inputted by scanning their bar-code. Since adjustments forms (AF1/2 where taxpayers change declared income) and other tax documents are not bar-coded a record of these is inputted manually in the system by entering the ID number of the taxpayer, the type of document received and the year of assessment. NAO suggests that IRD investigates the possibility of bar-coding adjustment forms and other similar documents so as to reduce the possibility of human error and make the process more efficient.

Apart from acknowledging documents this system groups the documents inputted in batches of not more than 30 documents. Each batch will be allocated a batch number and later a box number. This process enables the retrieving of particular documents in a simple and efficient manner. Any documents that are retrieved can be allocated a new batch number.

Each return inputted is then checked manually for completeness and if incomplete this is rejected. The reason for rejection is inputted in the acknowledgement system so as to be quoted in the rejection letter sent to the taxpayer.

Since tax returns filed online are acknowledged automatically and therefore no manual processing of these returns is needed, uptake of electronic lodgements by individuals should be increased. NAO therefore suggests that electronic lodgement through the web is marketed further so as to improve uptake especially for individual taxpayers. IRD may consider providing further assistance to taxpayers in the use of its web services. This service would also empower the taxpayer with the necessary knowledge to file their tax returns online unaided during the following years.

The NAO has observed that when a particular return is retrieved and would therefore need to be re-batched, the original batch number is no longer displayed by the system. The acknowledgement only displays the last batch number allocated to the particular document and therefore staff is unable to know the batch number that was originally allocated to that form. NAO suggests that this is amended in such a way that the system displays all batch numbers allocated to a particular document marking the last batch number as the current one. Such functionality should be made available to users with the required access levels as determined by IRD.

During the course of this audit, NAO noted that access to this application is assigned only to those users that are involved in the acknowledgement processes and rights may also be assigned depending on the user's role/section to acknowledge specific documents. Viewing of acknowledged documents is made through the return capture system.

NAO was informed that there are no pending bug fixes for this software application however there were two enhancements of a medium priority. These enhancements date back December 2010. NAO recommends that IRD and MITA should ensure that they are not dependent on any one particular person to provide support on the above-mentioned software application.

During the course of this audit NAO observed that each section is currently issuing its own management reports and submitting them to Management for evaluation. This process presents a risk of fragmentation of data. NAO thus suggests that the Acknowledgment system is enhanced so as to include a report generation facility through which Management can issue management reports on all sections rather than having sections issuing their respective reports and submitting them separately to Management.

3.3 Process Application

The Process Application System is used exclusively by staff at the computer section to trigger the batch processes done at the Inland Revenue including the generation and printing of returns, tax statements, PT and SSC claims and refunds. This application is only used by two specific officers and therefore has one access level.

This application is currently being re-written by MITA. A new version of this system has already been deployed at IRD. Staff is however still using the old system since some functions are as yet not available on the new version and therefore parallel running of both the old and the new version is required. IRD explained that new version is to incorporate all the currently used backend scripts.

The majority of functions available on the old version are not being used since these pertain to business processes which no longer exist.

Two pending enhancements of a low priority were reported to MITA in October and November of last year. Another pending enhancement required on the new system is the facility that would enable printing on A3 sheets. This facility is required so as to be able to print A3 statements.

The NAO observed that the printing of returns and other tax documents is generally carried out by one particular person. A call for applications for three to four additional employees was issued. NAO suggests that if new resources are engaged such a process is entrusted to at least two employees.

3.4 FSSFBT/FS7 Document Management

The FSSFBT and the FS7 Document Management systems are two separate modules used to generate requests for submission of FSS documents to employers, acknowledge and manage the documents received and process the FS3s and FS7s received both, in paper form or through IRD online portal.

Through the FS7 Document Management the user has the facility to view all the FS7s and FS3s sent by a particular employer since 1997. In cases when FS3 returns are not filed these can also be inputted by adjustments and afterwards compared with the ones which would eventually be filed. Whilst minor adjustments can be done by all users, the system only allows the super user to input major adjustments. NAO noted that when the Head of Section, who has super user rights assigned to her wants to issue a report detailing the adjustments made by her staff, she needs to select her staff from a whole list of IRD employees. This should be amended so that only the employees having access to this system are displayed in that list.

Access to these applications may be either view only or assigned depending on the user's particular role/section. The Head of Section has full rights to the system and allocates batches to particular users. The NAO has observed that when allocating batches, the super user needs to allocate each and every batch and cannot select multiple batches and allocate to a particular user all at once. The NAO therefore recommends that this function is incorporated in the system. Furthermore, NAO noticed that although the users can view the list of batches allocated to them by the super user and process them accordingly, the latter cannot view the list of pending batches that are allocated to a particular user. So as to be in a better position to assess the workload of each of the employees and the amount of batches processed, NAO recommends that the necessary functionality is added to the system so as to enable the head of section to keep track of the amount of batches that are still pending by any particular user.

The NAO has also noted that the Report Generator is not user-friendly and at times the reports available do not contain all the necessary information. Just to give one example, some reports do not display the batch number. Other reports are also giving the information needed in codes ex. EC3, EC7. These codes were set by ex-employees working in this section but since these employees are no longer available, the present staff is sometimes finding it hard to interpret such reports. NAO was however informed that MITA intended to revamp the report generator making use of business objects.

3.5 Audit Desktop

The Audit Desktop System is used by the tax audits section and by the TCU to initiate audits and keep track of the taxpayers under audit and of ongoing developments pertaining to such tax audits. Furthermore the system has an in-built calendar through which appointments with taxpayers are listed and appointment letters are sent. Appointment letters also indicate the documents that the taxpayer is to prepare for the meeting. Appointments can also be rescheduled or marked so as to indicate that the taxpayer attended. Notes may also be inputted so as to list any meeting notes. Moreover through this application the user can access the taxpayer's accounts. The audit desktop system also integrates with the return capture system so as to feed in the penalties that apply in each case.

This application was developed by MITA and deployed at the IRD in 2001. NAO was informed that the system was enhanced and a new version was deployed a few weeks before the audit.

This system has two main security functions, namely normal user and a supervisor. Access is assigned depending on the user's particular role.

During the course of this audit, NAO observed that when an enquiry/audit is opened the user is made to input the reasons for this enquiry. This same screen has the facility for the user to input remarks. NAO noticed that if any remarks are inputted these are not displayed anywhere through the system not even in the reports issued by the system. NAO thus suggests that IRD discusses this case with MITA so as to solve this issue.

NAO also noticed that the system sometimes loads certain years twice. Although this bug is not hindering the Department's operations in any way, NAO suggests that this is reported to MITA so it is solved avoiding the present inconvenience.

NAO observes that currently tax assessments are worked out manually and saved in the taxpayer's electronic folder residing on the server. Presently such documents are either held in the taxpayer's manual file or scanned and saved in the taxpayer's electronic folder saved on the server. IRD may also consider scanning these documents through the TPS system but restrict their availability to the staff working on that particular audit. NAO recommends that the IRD investigates the possibility of expanding this system's functionality so as to provide facilities through which:

- workings related to the tax assessments are stored in this system; and
- audit documents are scanned and images of these documents are saved in this system.

Chapter 4

Protection of Information Assets

Chapter 4 – Protection of Information Assets

4.1 Antivirus Software

Symantec Endpoint Protection (SEP) is installed on all the desktop computers and laptops at the IRD.

Besides a managed Antivirus (AV) and Anti Spyware (AS) product, SEP also provides several lines of defence through its managed Intrusion Protection System (IPS) and its managed firewall. Furthermore it provides Device and Application Control. All these features are instrumental in supporting the governance of ICT policies.

Moreover SEP prevents any endpoint from connecting to more than one network at any one time; thus eliminating the risk of network bridging.

This software is updated automatically by MITA.

Although MITA is responsible for providing all the necessary support, maintenance and updates with reference to SEP the NAO recommends that the IRD requests a periodic report (i.e. every six months) from MITA, so as to confirm that all computers within IRD are being updated. There may be instances whereby either because a computer is disconnected from the network or because of something malfunctioning, the updates pushed by MITA are not installed on a particular computer. The IRD should be in a position to periodically ensure that this is not occurring.

Furthermore, the NAO recommends that IRD requests a monthly report from MITA, that would indicate which computers were affected by viruses and if these viruses where cleared or not. This report would help the department identify and take any necessary actions needed in cases where the same computers are being affected by the viruses. This could be an issue of educating particular users as to what precautions could be taken so as these problems won't keep occurring and posing a risk to the Department's network.

4.2 Windows Server Update Services (WSUS)

As part of the support being provided by MITA, the Microsoft Software being used by the IRD is automatically updated through WSUS. WSUS is a locally managed system that works with the public Microsoft Update website to give system administrators more control by providing a software update service for Microsoft Windows operating systems and other Microsoft software. By using WSUS, MITA manages the distribution of Microsoft hot fixes and updates released through Automatic Updates to IRD's computers.

Although, as explained in the preceding paragraph, MITA is responsible for the distribution of patch updates to Microsoft Operating Systems and Microsoft-based Products to address identified vulnerabilities the NAO recommends that the IRD requests a periodic report (i.e. every six months) from MITA, so as to confirm that all computers within IRD are being updated normally. There may be instances whereby either because a computer is disconnected from the network or because of something malfunctioning, the updates pushed by MITA are not installed on a particular computer. The IRD should be in a position to periodically ensure that this is not occurring.

4.3 Electronic Mail, Internet Services and Wi-fi facilities

4.3.1 Electronic Mail & Internet Services

The NAO considers electronic mail (e-mail) and internet services as mission critical services especially in the case of IRD where a number of services are being offered online and the general public is being encouraged not only to use such services but also to use the Department's generic e-mail address for customer care and query purposes. E-mail and internet services can also be considered as principal vehicles for electronic communications both within IRD and with external entities.

In this regard, the NAO has observed that the IRD has adopted the e-mail and Internet Services policy that was issued by the former Central Information Management Unit .

During the course of this audit NAO has observed that as laid out in the above mentioned policy, IRD has implemented restrictions on both the e-mail and Internet Services. Filtering technology is being used so as to prevent internet access to illegal material and material which although not illegal may be harmful to society or may lead to loss of productivity. Moreover, e-mail messages in which the number of recipients exceeds 25 recipients are blocked. Furthermore, e-mail messages are also blocked if the size of the message is greater than 1.5Mb.

The NAO recommends that IRD periodically brings to the attention of its employees the salient points contained in this policy especially the Restrictions on use of e-mail and internet services as reproduced in Appendix D.

4.3.2 Wi-fi facilities

The IRD has a single wi-fi facility that is provided by MITA and deployed in a particular boardroom. Two specific laptops have access to this Wi-fi.

In this regard, the NAO has observed that the IRD has adopted the Government's Policy entitled GMICT Policy P 0047:2007 Wireless technology policy and directive.

4.4 Physical Security

4.4.1 Stored Documents

All incoming taxpayer correspondence is either captured or scanned and retained as images on the Department's data servers which are adequately backed up. However a few exceptions exist. In such cases, documents are stored in lock-up stores.

The NAO is informed that the Department is evaluating the possibility of processing such documents through the centralised document imaging system. The NAO thus suggests that in interim documents that are available in hard copy format are only stored in stores equipped with an intrusion detection system and smoke detectors.

4.4.2 Servers

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

4.4.3 Buildings

The NAO noted that the IRD has implemented a number of physical security measures throughout its buildings namely;

- A burglar alarm is installed in the – CLS.
- During peak periods, the cash office is manned by a member of the Revenue Security Corps. Another member of the Revenue Security Corps is stationed in Block 4.
- IRD's off-site storage facility is covered by security and is equipped with fire extinguishers.
- Structural alterations are currently underway in Block 1 in order to a receptionist desk at Ground Floor level.
- Movements of visitors to Block 2 are monitored by the messenger's office on both floors.
- Taxpayers visiting Block 3, Block 6 and Gozo office are escorted to the particular officer's desk.
- Taxpayers visiting the Department are normally directed towards the TPS section in Block 4 and the Cash Office at Block 5. These offices have purposely designed waiting and service areas.
- Visitors to the Tax Audits Section and TCU are required to register and sign at the reception area. Visitors are then escorted to the meeting rooms by the respective officers. Visitors are required to sign again when leaving the premises. A similar policy is applied at the International Tax Unit in Attard.
- Smoke detectors are installed at the computer section.
- Fire extinguishers are available throughout all IRD Blocks and offices, both in Floriana and Valletta and are checked on a regular basis.

The NAO thus suggests that IRD takes all the necessary measures to ensure that:

- an adequate level of intrusion and smoke detection is maintained; and
- the visitors policy adopted at the tax audits section and the TCU i.e. implementing a visitors register, is to be adopted throughout all IRD buildings

4.4.4 CCTV

The IRD also has a number of CCTV cameras installed in its buildings.

The NAO noted that CCTV recordings are saved on a hard disk which is physically located in the CCTV multiplexer. Multiplexers are mounted in the network cabinet of each respective block and these are locked. NAO suggests the security surrounding the networks cabinets is reviewed with the aim of introducing a higher level of access control to the area such as locking the rooms where these cabinets are held.

Access to live and recorded images is restricted to authorised personnel.

A CCTV system is also installed at CTD – Valletta offices. In this case the cameras located around the safe are physically monitored from a remote location during out-of-office hours.

Chapter 5

Risk Management, Business Continuity and Disaster Recovery

Chapter 5 – Risk Management, Business Continuity and Disaster Recovery

Although the IRD has discussed risk management, business continuity and disaster recovery, these plans have not been formalised. Such plans are still in draft form; IRD informed NAO that an initial draft shall be finalised shortly.

The NAO has however observed that although IRD has no formal plans, MITA has implemented measures so as to mitigate the risks involved in case of a total failure of IRD's systems. The IRD system is residing on two hosts, located in two different data centres. Data replication is handled by the database and occurs in real time, whilst files residing on the operating system are replicated twice daily using operating system commands. In case of a server failure, a manual process must be performed by MITA to switch the users to the other server (which is an identical replica). The estimated effort of switching users is 30 minutes.

The NAO thus suggests that a Business Impact Analysis and a Risk Assessment Exercise are carried out from which a Business Continuity Plan that includes a Disaster Recovery Plan is issued as detailed in Appendix D.

5.1 Business Impact Analysis

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

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

- Recovery Point Objective (RPO) - the acceptable latency of data that will be recovered ensuring that the Maximum Tolerable Data Loss is not exceeded.

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

After going through this process IRD should then determine its recovery requirements which will consist of the business and technical requirements for recovery of the critical function.

5.2 Risk Assessment Exercise

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

NAO recommends that IRD undertakes a risk analysis exercise that would take into account all types of threats that can impact IRD's business. Fires, floods, acts of sabotage, hardware / software failures, virus attacks, cyber crimes and internal exploits are all examples of the types of events that are to be analysed assigning a probability assessment value to each.

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

5.3 Business Continuity and Disaster Recovery Plans

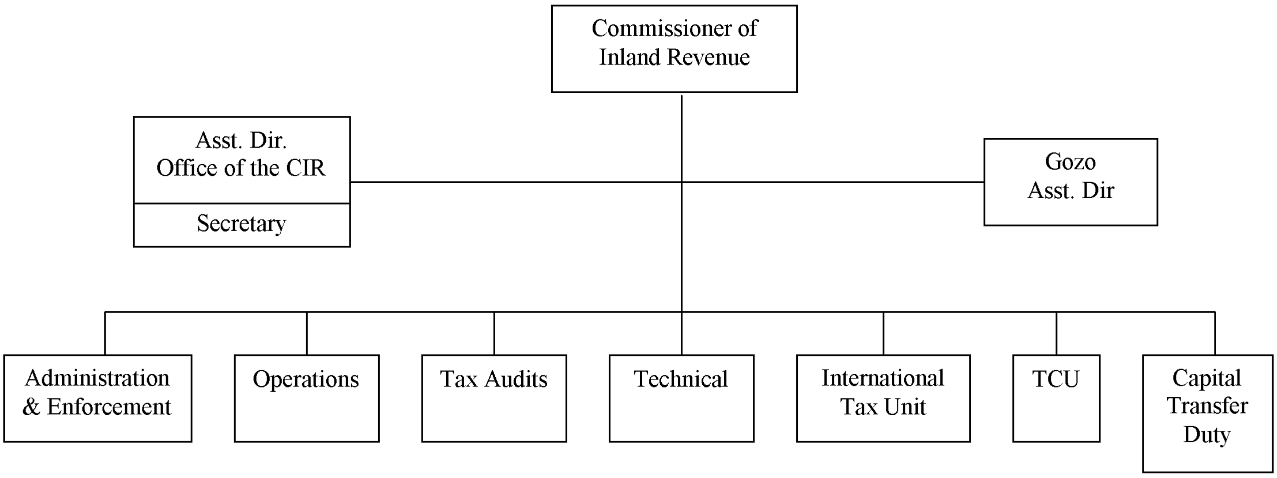
The Department should also have a business continuity and disaster recovery plan designed to reduce the impact that disruptions might inflict on the Department's operations.

Moreover, the Department should ensure that the Service Level Agreements it has with its suppliers cater for adequate and timely maintenance, support and business continuity.

Appendices

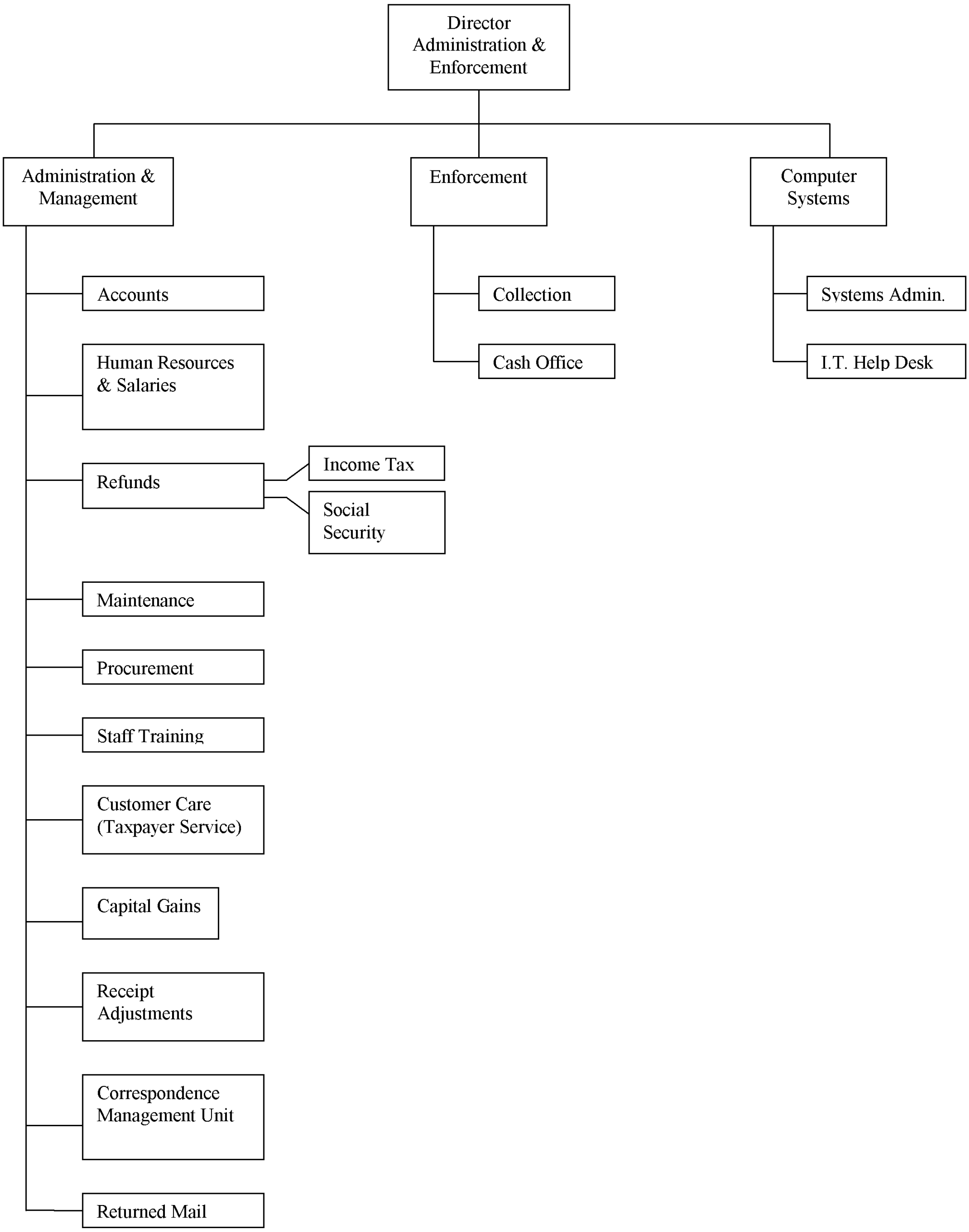
Appendix A – ORGANISATION CHARTS[3]

Inland Revenue Department

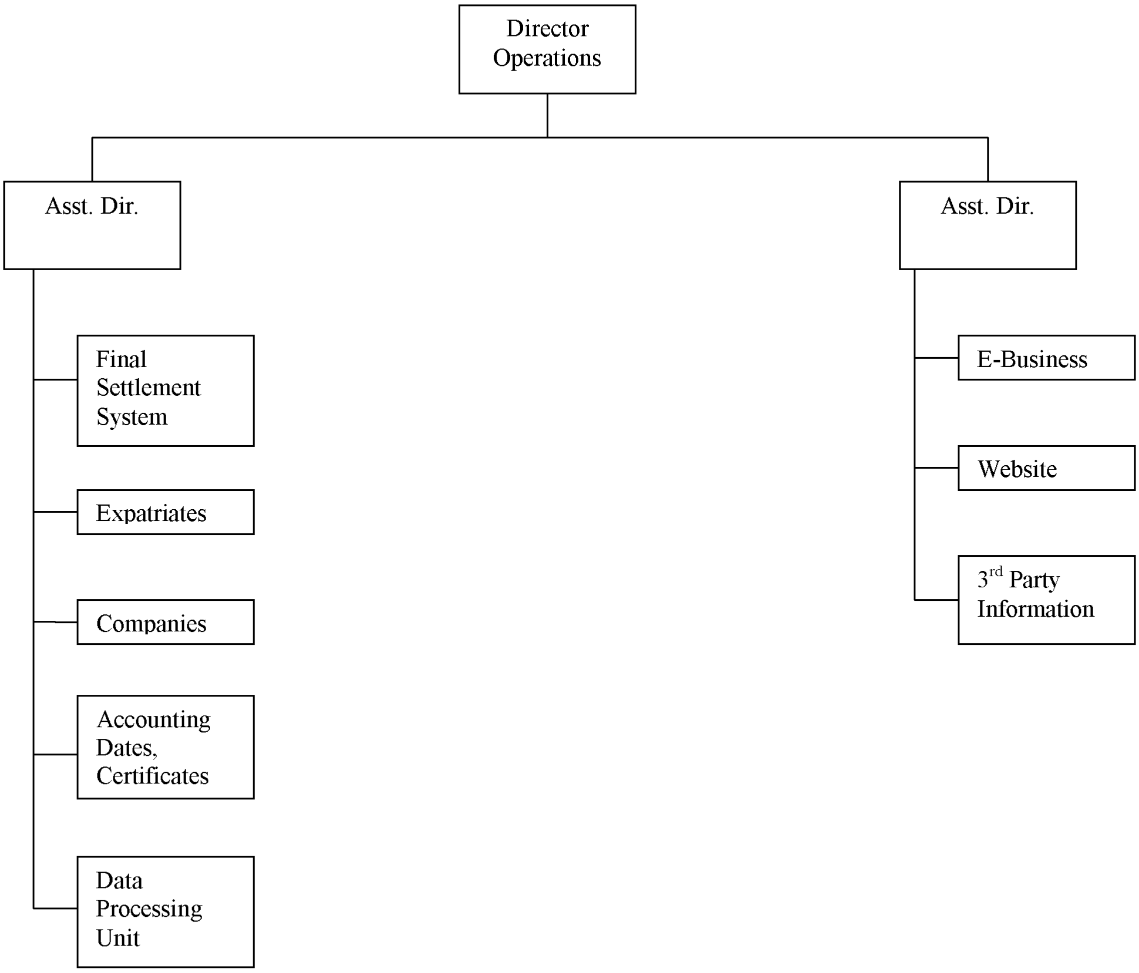


[3] The Organisation Charts in Appendix A have been provided by IRD.

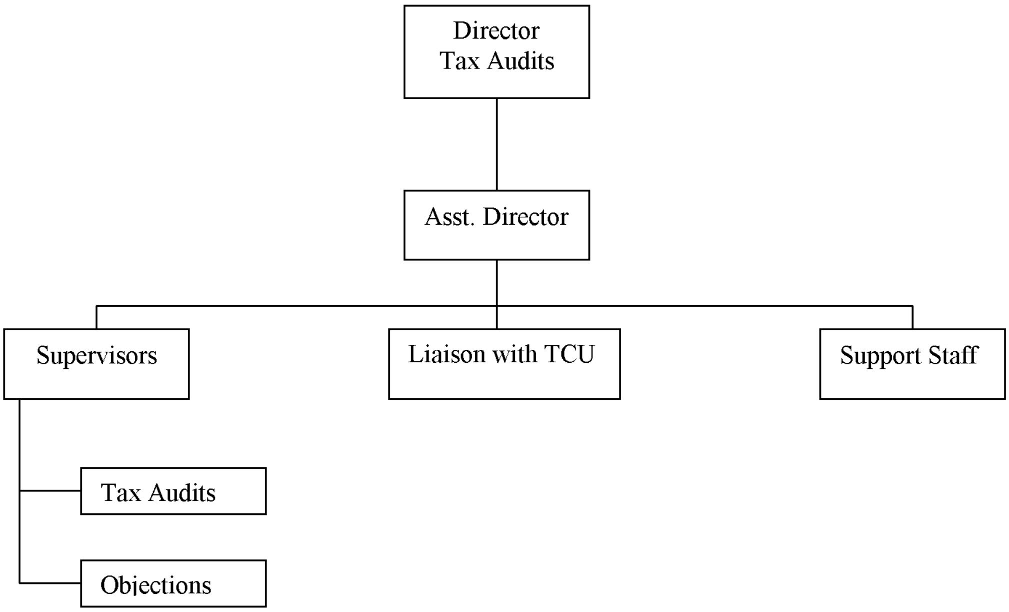
Administration & Enforcement



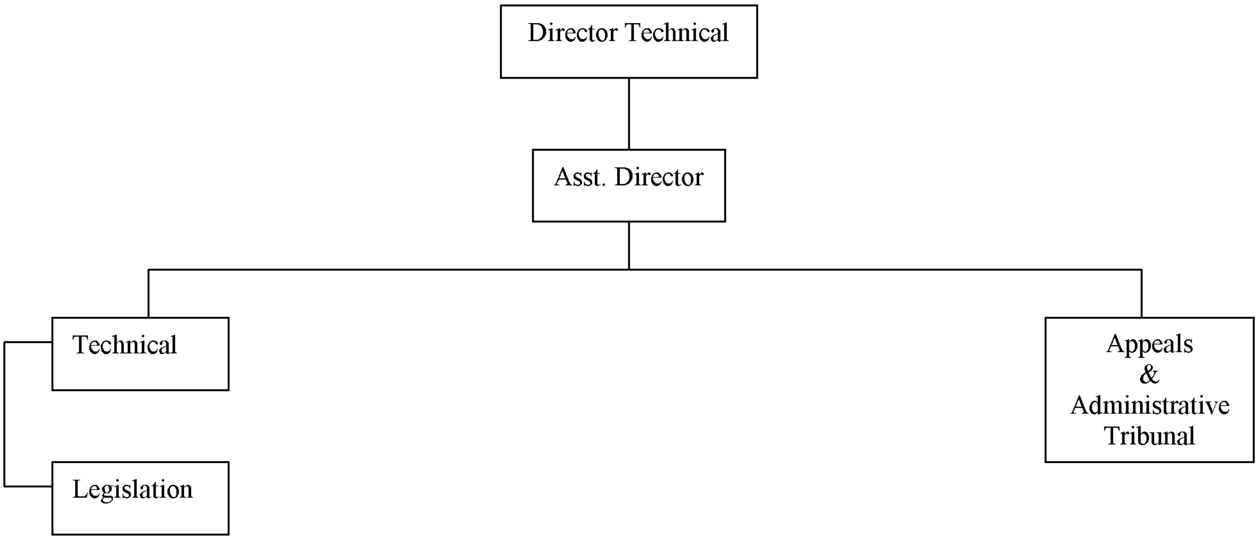
Operations


Director Operations
Asst. Dir.
Asst. Dir.
Final Settlement System
Expatriates
Companies
Accounting Dates, Certificates
Data Processing Unit
E-Business
Website
3rd Party Information

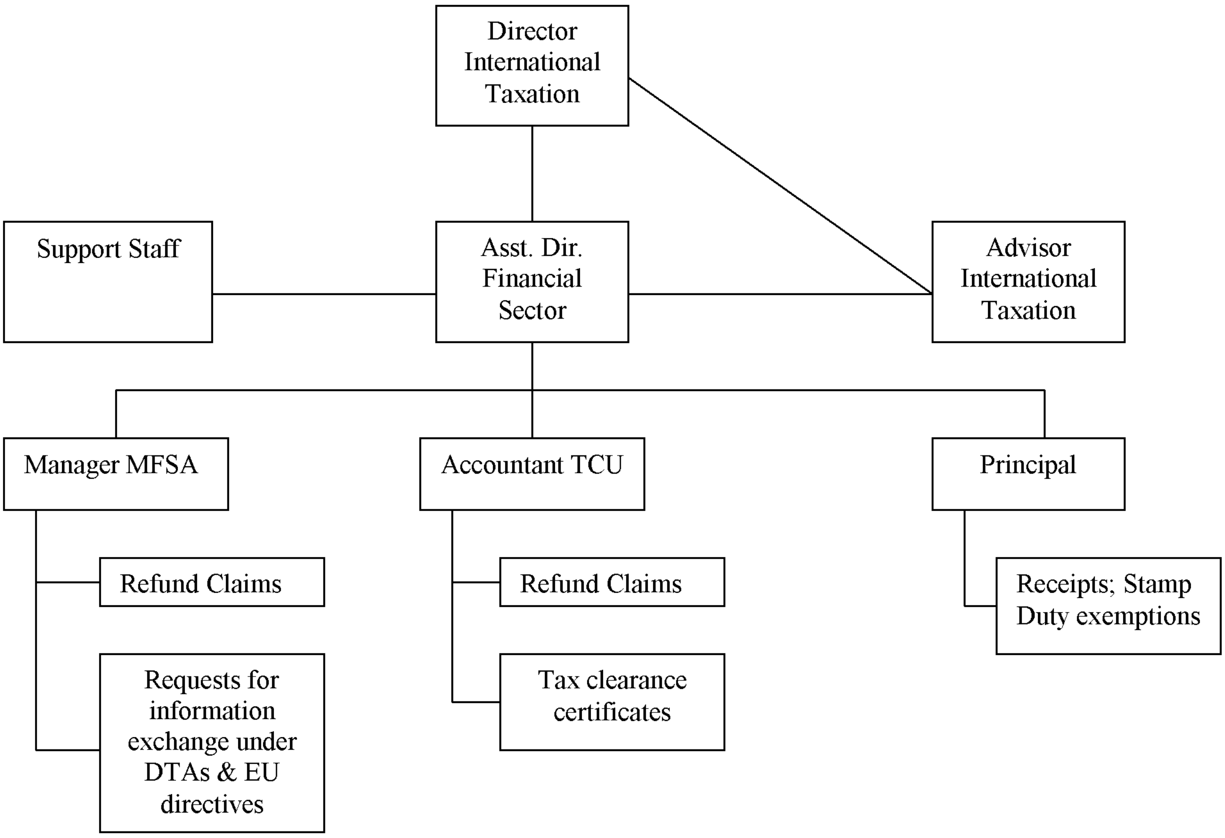
Tax Audits


Director
Tax Audits
Asst. Director
Supervisors
Liaison with TCU
Support Staff
Tax Audits
Objections

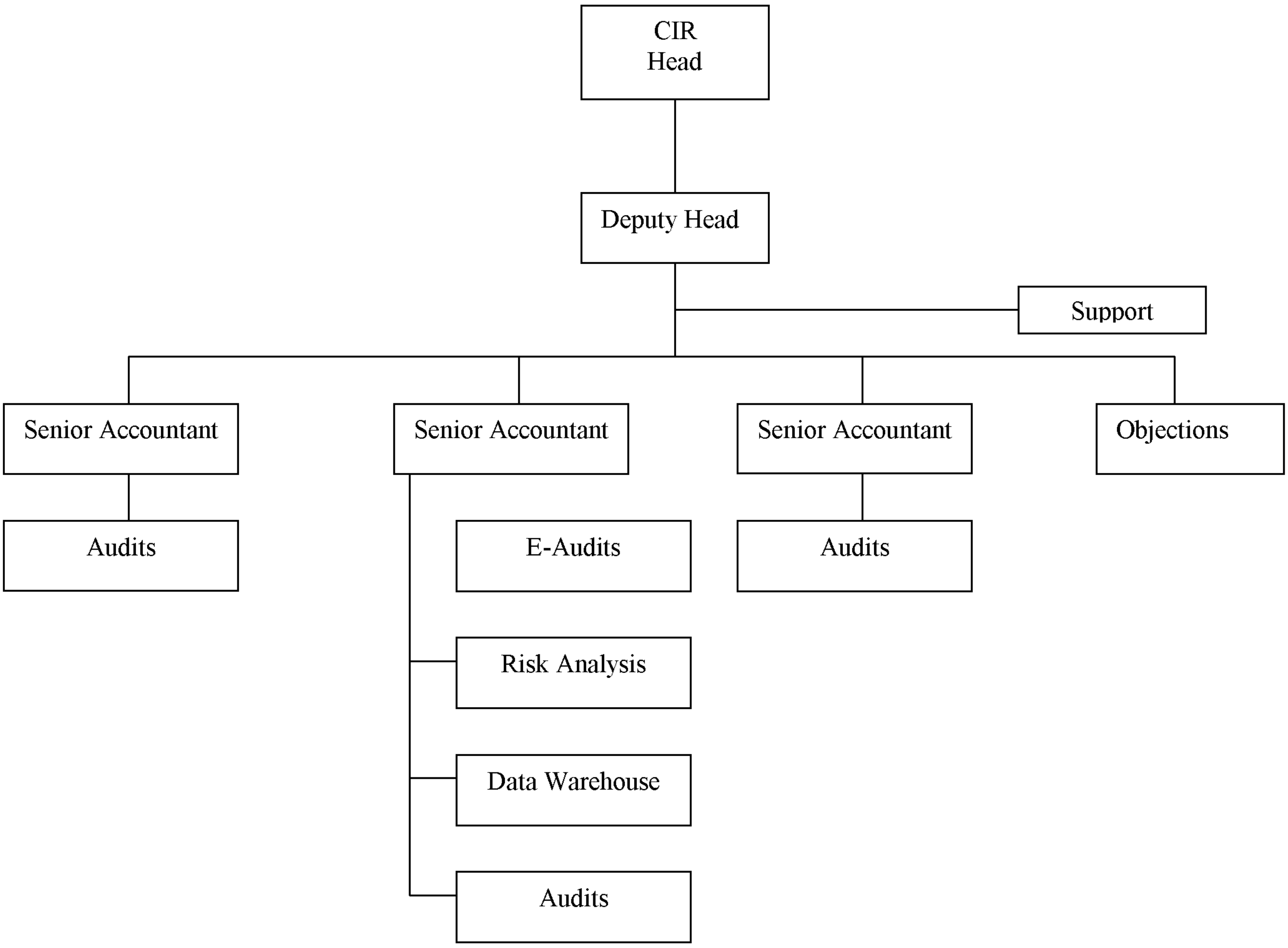
Technical


Director Technical
Asst. Director
Technical
Legislation
Appeals
&
Administrative
Tribunal

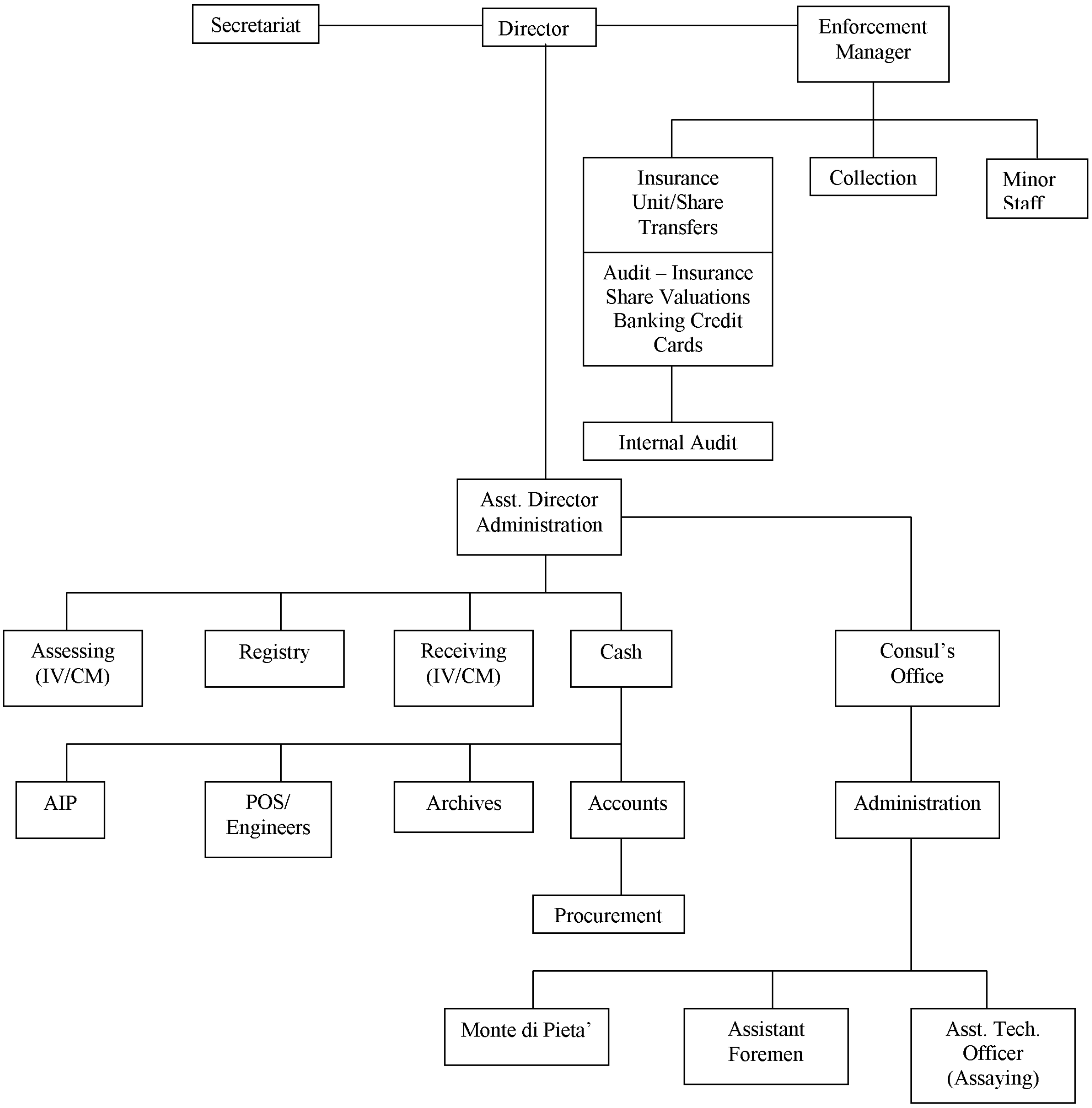
International Tax Unit


Director International Taxation
Support Staff
Asst. Dir. Financial Sector
Advisor International Taxation
Manager MFSA
Accountant TCU
Principal
Refund Claims
Requests for information exchange under DTAs & EU directives
Refund Claims
Tax clearance certificates
Receipts; Stamp Duty exemptions

Tax Compliance Unit



Capital Transfer Duty



Appendix B – Controls

General Controls are controls embedded in IT processes and services, whilst controls embedded in business process applications are commonly referred to as Application Controls.

Controls that were considered during this audit are:

- **General Controls:** Systems development, Change management, Security and Computer operations
- **Application Controls**: Completeness, Accuracy, Validity, Authorisation and Segregation of duties

For application controls, CoBit lists six recommended objectives[4] as follows:

- **AC1**: Source data preparation and authorisation - Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Errors and irregularities must be detected so they can be reported and corrected.

- **AC2**: Source data collection and entry - Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input are performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, original source documents should be retained for the appropriate amount of time.

- **AC3**: Accuracy, Completeness and Authenticity checks - Ensure that transactions are accurate, complete and valid. Validate and edit, or send back for correction, input data as close to the point of origination as possible.

- **AC4**: Processing Integrity and Validity - Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transaction does not disrupt the processing of valid transactions.

- **AC5**: Output review, Reconciliation and Error Handling – Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient and protected during transmission, that verification, detection and correctness of the accuracy of output occurs; and that information provided in the output is used.

- **AC6**: Transaction Authentication and Integrity: Before passing transaction data between internal applications and business/operational functions (in or outside the enterprise), check it for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.

[4] Application Controls ITGI, 2007a, CoBit 4.1 as per www.itgi.org

Appendix C – Restriction on use of E-mail and Internet Services

Restriction on use of e-mail:

□ Impersonate or forge the signature of any other person when using e-mail.

□ Amend messages received in a fraudulent manner.

□ Gain access to, examine, copy or delete another person's e-mail without the necessary authorisation from the person concerned.

□ Disclose their password or other means of access.

□ Use someone else's password or other means of access in a computer.

□ Use e-mail to harass or defame any person or group of persons.

□ Use e-mail to conduct any personal business or for commercial or promotional purposes.

□ Send as messages or attachments items that may be considered offensive, pornography, illegal material, chain letters, or junk mail.

□ Send e-mail in bulk unless it is formally solicited.

□ Place Government-assigned e-mail address on non-official business cards.

□ Send trivial messages or copy messages to people who do not need to see them.

□ Send unsolicited mass e-mailing to more than 25 e-mail users, if such unsolicited e-mailing provoke complaints from the recipients.

□ Use the service of another provider, but channelling activities through a MAGNET account as a re-mailer, or use a MAGNET account as a mail drop for responses.

Restriction on use of internet services:

□ Download files from the Internet without adhering to existing policies on virus control.

□ Download material (including software) that is not work-related.

□ Enter into any contract over the Internet without approval from the appropriate Head of Department or his/her delegate.

□ Use the Internet to conduct any personal business or for personal commercial purposes.

□ Post a single article or advertisement to more than ten Usenet or other newsgroups, forums, e-mail mailing lists or other similar groups or lists.

□ Post to any Usenet or other newsgroup, forum, e-mail mailing list or other similar group or list articles, which are off-topic according to the charter or other owner-published Frequently Asked Questions (FAQ) or description of the group list.

Appendix D – Business Continuity and Disaster Recovery Plan

A Business Continuity Plan should:

- include a list of essential hardware, software and information;
- state whether the Department has an alternate site from which to resume operations;
- preferably include details of manual processes that could temporarily maintain operational functionality for each business process in the event of a total IT system collapse;
- include a Disaster Recovery Plan that amongst others lists the access rights granted following a restore;
- include a restoration plan that details how to return operations to normality whether in a restored or in a new facility;
- be periodically tested and updated;
- be stored in hard-copy and soft-copy format both on-site and off-site; and
- be distributed to members of staff, Head of Sections etc.

Furthermore the Disaster Recovery Plan should stipulate the procedures that are to be taken in the event IT facilities become inoperative due to extreme incidents. It should also document the recovery approach and the recovery time objectives.

Recent NAO Publications

NAO Work and Activities Report

January 2011	Work and Activities of the National Audit Office 2010

NAO Audit Reports

February 2011	Performance Audit: Renewable Energy in Malta Follow-up
March 2011	Performance Audit: Road Surface Repairs on the Arterial and Distributor Road Network
April 2011	Performance Audit: Achieving a Healthier Nutrition Environment in Schools
May 2011	Enemalta Corporation Tender for Generating Capacity (Supplementary Investigation)
June 2011	Performance Audit: Flexible Work Arrangements for Public Employees
July 2011	Performance Audit: Dealing with Asylum Applications