N A O
National Audit Office
MALTA

IT Audit:
Active Ageing and Community Care
Ministry for Active Ageing

February 2023

N A O
National Audit Office
MALTA

Information Technology Audit
Active Ageing and Community Care
Ministry for Active Ageing

Report by the Auditor General
February 2023

Table of Contents

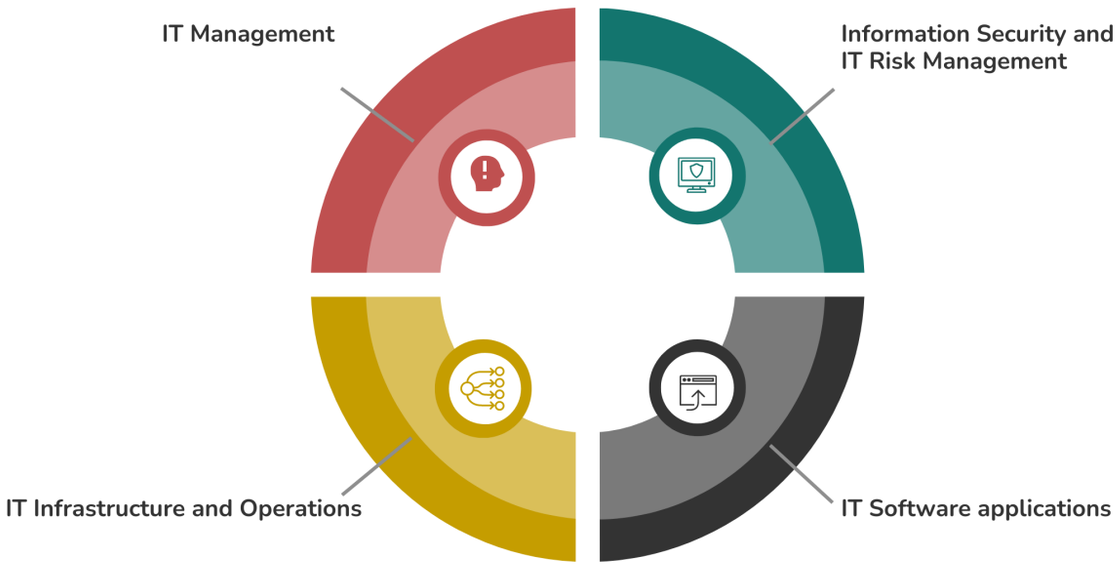
List of Tables and Figures

List of Abbreviations

The following is a list of abbreviations used throughout this report:

AACC	Active Ageing and Community Care
AMS	Asset Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CCTV	Closed-Circuit Television
CdB	Common Database
CDR	Corporate Data Repository
CEO	Chief Executive Officer
CIO	Chief Information Officer
COBIT	Control Objectives for Information and related Technology
CPAS	Clinical Patient Administration System
DRP	Disaster Recovery Plan
GMICT	Government of Malta ICT
ICM	iSoft Clinical Manager
ICT	Information and Communications Technology
IMU	Information Management Unit
ISACA	Information Systems Audit and Control Association
IT	Information Technology
LAN	Local Area Network
MAGNET	Malta Government Network
MFAA	Ministry for Active Ageing
MITA	Malta Information Technology Agency
MSCA	Ministry for Senior Citizens and Active Ageing
MSPC	Ministry for Social Policy and Children's Rights
NAO	National Audit Office
OPM	Office of the Prime Minister
SABS	Sistema għall-Amministrazzjoni tal-Benefiċċji Soċjali
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
VPN	Virtual Private Network

Key Recommendations



Chapter 2 - IT Management

- Draft an IT strategic plan.
- Formalise further the data wiping process within the IT equipment disposal procedure.
- Ensure that the service agreement covering the AACC's legacy core system (CCG) is terminated once the system is completely replaced.
- Recruit additional IT officers.

Chapter 3 - IT Infrastructure and Operations

- Install temperature/ humidity monitors, smoke detectors as well as improve cable management in network rooms at the Valletta and Qormi AACC offices, where necessary.
- Install air-conditioning at the AACC Valletta office network room.
- Clearly define responsibility for regular backups, testing of restores and audit trails of the new CMS in the related service agreement once the new system is fully implemented.
- Ensure regular backup of offline mailboxes of both AACC user and generic email accounts.
- Review current list of generic email accounts.

Chapter 4 - IT Software applications

- Clearly define responsibility for system administration/operations and backup/restore processes for the new CMS in the related service agreement, once the system is completed.
- Discuss and address any adjustments that may be required to ensure adequate performance levels when the new CMS is working at full load.
- Restore broken and missing links within the AACC website and conduct a periodic review of the website.

Chapter 5 - Information Security and IT Risk Management

- Clearly outline the responsibility for anti-malware and anti-virus protection at a server level in the related service agreement once the new CMS is completed.
- Conduct an IT business impact analysis and draft a Business Continuity Plan with a Disaster Recovery Plan.
- Draft an information classification policy.
- Review physical access controls at all AACC premises including the residential homes and day care centres, to manage physical access to IT assets on site.

Executive Summary

The scope of this Information Technology (IT) audit was to analyse the IT systems and infrastructure utilised by the Active Aging and Community Care (AACC) in Malta. In this context, this audit essentially sought to determine whether the AACC had the necessary controls in place to maintain the confidentiality, integrity and availability of data, ensure the efficient use of IT resources, as well as to identify any potential risks and make the necessary recommendations to mitigate such risks.

Key Findings and Recommendations

Following the background information on the AACC and overall structure of this report, provided in Chapter One, the following Chapter covers areas related to ICT governance, support, and training. The following are the key findings and recommendations included in Chapter Two:

- Whilst acknowledging the considerable efforts being undertaken by the AACC in the area of IT management and development, notwithstanding the need of additional resources in this important area, the NAO noted that the ACCC does not yet have a formal IT strategic plan and recommended that such a plan is drafted, which would include plans of all major IT projects proposed by the AACC/Ministry/IMU.

- Though the NAO was pleased to note the AACC's procedure for IT equipment disposal, this Office made some recommendations to formalise further the data wiping process forming part of the procedure.

- Given that one of the AACC's key software applications (CCG system) is in the process of being replaced, the NAO recommended that the AACC ensures that the related service agreement is terminated once the system is no longer in use. With regards to the agreement related to the AACC website, the Office recommended that the document is more readily available for audit purposes.

- The NAO noted the urgent need for additional IT officers in order to reduce the dependency on one official and ensure proper segregation of duties. Otherwise, timely implementation of all our recommendations would be extremely difficult, if not outright impossible.

Chapter Three of the report covers the IT infrastructure setup at the AACC, and reviews other key aspects of its IT operations. The following are the key findings and recommendations:

- In view of security issues, the NAO noted the lack of temperature and humidity monitoring equipment in the network rooms at the AACC offices in Valletta and Qormi and recommended that such equipment is installed. Furthermore, this Office recommended that the AACC ensures

that all its network rooms are equipped with smoke detectors as some did not have such devices. The NAO also recommended that the AACC should ensure that proper cable management and housecleaning is maintained in all network rooms of the AACC Valletta and Qormi offices. With reference to the network cabinet in the Valletta office, the NAO recommends that the area is equipped with air-conditioning, cleared of stored files/documents in the vicinity and has its physical access limited to authorised staff only.

- The NAO recommends that the AACC ensures that the responsibility for regular backups, related testing of restores and audit trails of the new AACC primary system currently being developed, are clearly defined in the service agreement once the new system is fully implemented and commissioned.

- With reference to the offline mailboxes, both the AACC user and generic email accounts are backed up on a regular basis, as recommended by the NAO. The use of certain generic email accounts should be reviewed, as some were last used in July 2020. The AACC should also consider the option of archiving in order to reduce the size of some of the generic mailboxes.

Chapter Four includes a review of the AACC Case Management System, as well as the Entity's website and social media. The key findings and recommendations included in this Chapter, included amongst others the following:

- With reference to the new AACC CMS system being implemented, the NAO recommended that the AACC ensures that:

    - roles and responsibilities associated with system administration/operations and backup/restore processes are to be clearly defined in the related service level agreement to be signed once the new AACC CMS system is fully commissioned;
    - future backups are stored off-site in an adequate secure place;
    - meetings with the IMU-MSPC and the software developer are held to discuss system/infrastructural adjustments that maybe required to ensure continuous availability and adequate performance levels when the system is working at full load (i.e. being accessed by circa 600 AACC users across the various services that the Entity offers);

- The NAO recommended that the AACC takes the necessary steps to ensure that all broken and missing links within the AACC website are restored. A periodic website review to ensure that the web content remains updated, was also recommended by this Office.

Chapter Five of this report looks at the Information Security and IT related risk management at the AACC. The following are the key findings and recommendations:

- With regards to measures to protect from software viruses and malware, the NAO recommended that any service level agreement covering the support and hosting of the new AACC CMS system should clearly outline the responsibilities for anti-malware and anti-virus protection at a server level.

- The NAO recommended that the AACC conducts an IT business impact analysis in order to draft the related Business Continuity and Recovery Plans which the Entity did not have.

- It was observed that the AACC did not have an information classification policy, which defines the security levels for data based on data sensitivity, value and criticality. The NAO therefore recommended that the AACC should draft such a policy.

- The NAO recommends that the AACC reviews the physical access controls present in all its premises, including the residential homes and day care centres, in order to ensure the current measures are adequate and updated with the use of current technology. Furthermore, this Office also recommended that the AACC carries out regular reviews of the fire detection and suppression systems in all of the Entity's sites.

Overall, the NAO commends the fact that the AACC is investing in a holistic project for the creation of a new digital platform and the adoption of a new software application which will cover the majority of AACC services.

Chapter 1| Introduction

This Chapter provides background information on the subject under review and sets the context for the audit. It details the audit scope and objectives, and describes the audit methodology followed in attaining them, and concludes with a brief overview of each Chapter in this report.

1.1 Background

Mission statement

The aim of the Active Ageing and Community Care (AACC), as stated on its website's landing page, is to help people stay in charge of their own lives for as long as possible as they age, and to offer opportunities for older adults to remain physically, mentally and socially active. It defines its fundamental key values around three aspects: a society for all ages, intergenerational equity, and empowerment[1]. In this context, the AACC states that it's role "*is to be partners with the elderly and society through holistic client-oriented policies and support so that elderly people continue to enjoy life to their maximal potential in their individual settings*."

Functions and responsibilities

The Entity focuses on providing numerous community services, broadly categorised into community clinical services, and other non-clinical community services. Community clinical services encompass the provision of amenities, such as community geriatrician services, community psychogeriatric consultation service, and (day/night) dementia activity centres, amongst others[2]. Meanwhile, several other amenities are grouped under other non-clinical community services, the most notable being, active ageing centres, carer at home scheme, and continence service[3].

Clients/customers

All the services offered by the AACC are intended to cater for the elderly citizens in Malta and Gozo.

[1] https://activeageing.gov.mt/?lang=en
[2] https://activeageing.gov.mt/community-clinical-services/?lang=en
[3] https://activeageing.gov.mt/what-we-offer/other-community-services/?lang=en

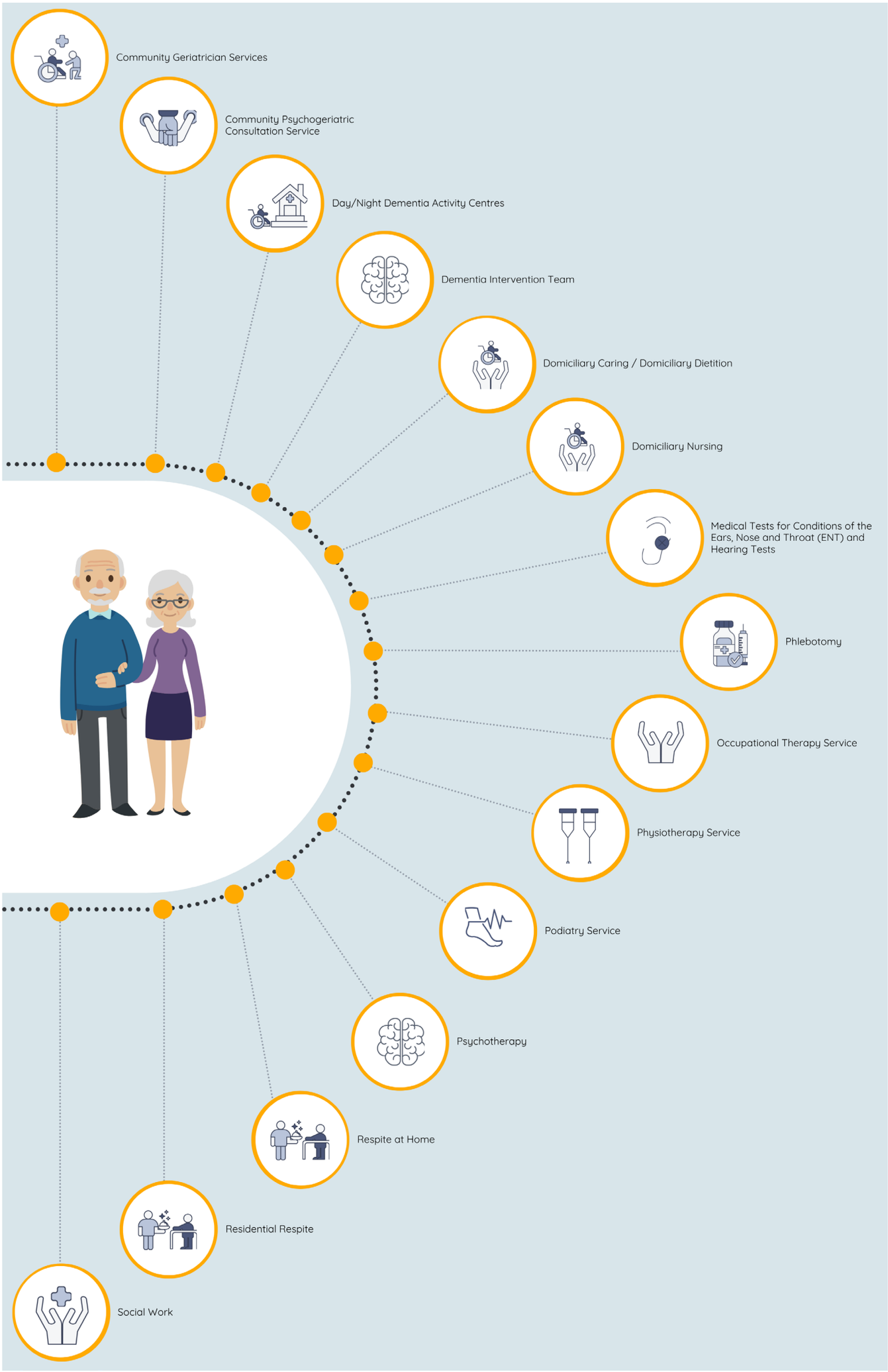


Figure 1 - AACC Community Clinical Services

Organisation structure/role

The AACC forms part of the Ministry for Active Ageing (MFAA), previously referred to (or known) as the Ministry for Senior Citizens and Active Ageing (MSCA). The Entity is headed by a Chief Executive Officer, who answers directly to the Ministry's Permanent Secretary.

Recent investments

In terms of Information and Communications Technology (ICT) investment, and adoption of new technologies, the AACC is currently investing in a holistic project, which will see the creation of a new digital platform and the adoption of a new software application. This software application will see the majority of AACC services being based on this new digital platform once this project is completed. In fact, the AACC has reported that a number of modules, each related to specific AACC services, have already been completed. Meanwhile, as part of another initiative, the AACC had in March 2021 installed free Wi-Fi access in all homes and made it available in each and every room. The NAO acknowledges the efforts being undertaken by the AACC in order to enhance IT management and development.

In this context, this Information Technology (IT) audit sought to examine the current state of the ICT within the AACC to identify any potential risks, and through this report, document the observations, and make the necessary recommendations to mitigate those risks. All resulting findings and recommendations are contained within this report, issued by the IT Audits and Operations Unit within the National Audit Office (NAO). Eventually, the AACC Management could then address and tackle the issues raised and highlighted by this Office in this report, mainly by implementing suitable remedial measures, in line with, or surpassing, the recommendations put forward by the NAO in this report.

1.2 Organisation Structure

The AACC carries out its administrative operations primarily from two buildings. The main offices are located above a third-party offices in Qormi and are spread over two floors. These offices house the majority of the AACC's staff, both administrative and clinical, and are the backbone of the Entity, where processing of the majority of applications, and related cases, in relation to services provided, is carried out.

The AACC also has a smaller office situated in Valletta. These premises, known as *Ċentru Servizz Anzjan*, are located on the ground floor directly underneath the offices of the Ministry for Finance and Employment, housed within the same building. These offices serve as the front office of the Entity, where the majority of applications submitted to the AACC are initially received, although some services are also offered from here. The Entity's administrative staff posted here are mainly responsible for the initial processing of these applications, before being forwarded to the AACC offices in Qormi for further handling.

In the meantime, the AACC also operates four Government owned Residential Care Homes, located at Mellieħa, Mtarfa, Mosta, Floriana, as well as 11 Day Centres spread around various locations in Malta, namely Mellieħa, Dingli, Żurrieq, St Luċia, Żejtun, Birżebbuġia, Bormla, Sliema, Ħamrun, St Venera, and

Mosta. The latter, enable senior citizens with opportunities, through various activities organised during the day, to remain physically, mentally and socially active.

Similarly, the AACC also operates Dar Padova in Għajnsielem, Gozo, through which a number of services, including night shelter and dementia related services, are offered to Gozitan residents. Similar services are also offered through the Dementia Centres operated from Safi and Mtarfa, the latter forming part of the Mtarfa Residential Care Homes.

Finally, the AAAC also has a stores facility likewise located within the Mtarfa Residential Care Home.

In terms of setup[4], at a high level, the AACC is split into three branches, encompassing Community Services, Residential Care, and the Administration These are further split into various units covering each of the services being offered by AACC, as indicated earlier on in this Chapter.

Each of these branches fall under the direct responsibility of a senior managerial officer (Assistant Director, Senior Manager, Chief Nursing Manager, or other senior official), all of whom answer directly to the Chief Executive Officer, AACC.

In terms of client feedback, the AACC informed the NAO that a simple survey kiosk, is installed at *Ċentru Servizz Anzjan* in Valletta. The survey kiosk gathers basic user feedback through three 'smiley' faces (happy, passive, sad). The survey kiosk is owned by the People and Standards Division within the Office of the Prime Minister (OPM), and the survey results are received directly by the aforementioned Division. A monthly spreadsheet report with the final results is forwarded to the AACC by OPM. In this regard, the AACC stated that there were 46 clicks during the sample audit period (April 2022).

1.3 Workforce Distribution and Work-Life Balance Measures

The total AACC workforce is made up of over 800 employees, of which, 353 are based at the AACC Head Office and Community. The remaining employees, over 320 work within the four Residential Care Homes, less than 80 are shared between the eleven Day Centres, over 50 in the three Dementia Centres, and 12 officers are posted at the Stores.

The total AACC workforce[5] as at audit date, can be classified as follows:

[4] The AACC organisation chart, as at Q1 2022, is annexed in Appendix A.

[5] The total AACC workforce quoted includes staff engaged/contracted through third-party agencies.

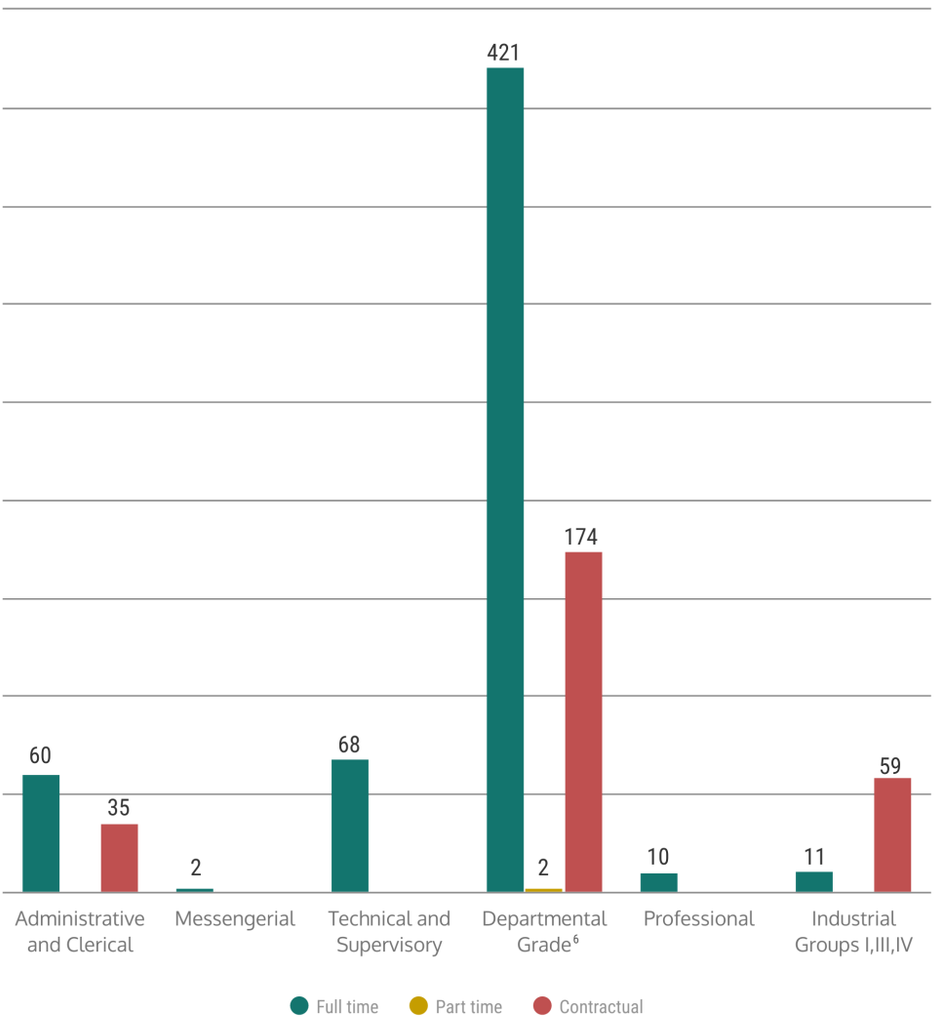


Figure 2 - AACC Workforce

As shown in Figure two above, the vast majority of AACC employees are engaged on a full time basis, whilst a substantial portion of the AACC workforce has been engaged/contracted through third-party agencies.

Post COVID-19 pandemic, family-friendly, flexible work arrangements are also being availed of by a number of AACC employees. The AACC employees availing themselves of such arrangements, as at audit date, are as follows:

Reduced Hours	Remote (Tele) Working
69	59

Table 1 - Flexible Work Arrangements

[6] Departmental Grades within AACC include various grades including, amongst others: Allied Health Professionals, Allied Health Practitioners, Nursing Managers, Charge Nurses, Staff Nurses, Enrolled Nurses, Social Workers, Practice Nurses, Care Workers, Nursing Aides, etc.

In order to ensure that employees can easily working remotely, all officers who are benefitting from family-friendly flexible work arrangements are primarily provided with laptops, as well as a mobile phone, with internet, for those under a remote working agreement. The latter can be used for authentication and booking purposes, using the Remote Workspaces facility.

Remote working employees were also given access to a Virtual Private Network (VPN) facility provided by the Malta Information Technology Agency (MITA), through the FortiClient VPN software, thereby enabling secure access to key AACC systems from outside the office premises. Such systems include the new AACC Case Management System, as well as Sistema għall-Amministrazzjoni tal-Benefiċċji Soċjali (SABS), Clinical Patient Administration System (CPAS), and Microsoft Teams.

Furthermore, phone calls to office telephone lines are automatically diverted to the portable devices (laptops and/or mobile phones), through the use of the Rainbow application, which is configured such that officers working remotely can phone and receive calls, through the office telephone line, using their portable devices (office laptop or mobile phone) from home.

Meanwhile, printing facilities can be accessed by remote working employees by going to any nearby remote working hub. However, it is to be noted that official physical documents and files are not taken outside office premises by remote working employees.

1.4 Legislation

The AACC operates within the context of the Social Security Act (Chapter 318)[7], as well as the State Financed Residential Services Rates Regulations (Subsidiary Legislation 318.13[8], as established by Legal Notice 151 of 2018[9], and previously Legal Notice 259 of 2004[10]). This legislation provides parameters which are used to professionally assess applications submitted, and to apply fees and charges due for services availed of by the applicant, where applicable.

1.5 Audit Scope and Objectives

The scope of this IT audit was to analyse the ICT and the management and governance of IT, within the AACC, in a number of key IT areas defined further down below. Public funds used by the AACC in these key IT areas can be characterised as Government investments, which were thus scrutinised, in a risk-based manner, to determine whether the necessary level of controls exist, at Entity level, so as to ensure that assets are safeguarded, resources are used efficiently, data integrity is maintained, and organisational goals can be achieved effectively.

[7] https://legislation.mt/eli/cap/318/eng
[8] https://legislation.mt/eli/sl/318.13/eng
[9] https://legislation.mt/eli/ln/2018/151/eng
[10] https://legislation.mt/eli/ln/2004/259/eng

In line with this scope, this IT audit sought to review and assess the level of controls in place, including those relating to the following key IT aspects, namely, IT management, IT infrastructure (including network infrastructure), IT operations, and Information security and software applications, amongst other key areas.

Furthermore, the current state of the AACC's IT operations and systems were reviewed at a high level so as to elicit any potential areas of risk to the Entity, its functions and operations, and/or its clients.

Therefore, through this report, the primary objectives were to document and summarise all the information gathered from various sources and identify any areas of concern; determine whether the AACC's IT setup facilitates operations in an effective, efficient, and economical manner; list all the observations, findings and any potential risks identified; and make the necessary recommendations to mitigate those risks.

Notwithstanding the above, it is to be noted that, given the aforementioned scope, the review of the selected software application/s does not constitute an in-depth information systems audit, which mandate would typically be carried out as a stand-alone review of a given information system.

1.6 Audit Methodology

In the period prior to undertaking this assignment, audit research was conducted gathering and assessing any publicly available information, from various sources, on the subject matter. Having defined the scope of the exercise and formulated an audit plan, an overview of the IT audit process was outlined, through an introductory meeting held with AACC senior management. A request for preliminary information and data was also made by the NAO and forwarded to the auditee.

Subsequently, a number of on-site meetings whereby the NAO audit team were briefed on the main operations, functions and processes adhered to by the Entity, followed by a familiarisation walkthrough to acquaint themselves with the AACC's setup and operating environment on a first-hand basis, from an IT perspective.

The compilation of an in-depth IT audit questionnaire by the NAO audit team ensued, and eventually completed by the AACC. The documented response provided comprehensive insight, and further enhanced the audit team's understanding of the IT setup and operating environment at the AACC.

Following an internal risk analysis and review of available information and feedback submitted, audit testing commenced. As already highlighted, the NAO's testing was segmented so as to verify and assess various aspects of IT within the AACC. This included, IT management (including IT strategy, objectives, internal structures, etc.), IT infrastructure (such as firewall and network protection, etc.), IT operations (including IT functions and processes), Information security (including operating system patches and updates, anti-virus, anti-malware and threat protection updates, etc.), and software applications (such as login credentials, audit trails, data backups, and data confidentiality, etc., and software usage and objectives) amongst other areas.

Notwithstanding the above, it is to be noted that the NAO's audit team had to rely heavily on the documentation and any additional information provided by the auditee, as well as numerous online meetings and correspondence, whilst keeping on-site audit fieldwork (physical verifications, meetings and interviews) to a minimum. This was done so as not to disrupt the hectic operations of the Entity, given, in particular, the ongoing development, testing and implementation of a new, key IT software application, overrunning the audit period.

Furthermore, as far as possible, the methodology adopted by the NAO relied on the Control Objectives for Information and related Technology (COBIT) set of best practice guidelines[11], created by the Information Systems Audit and Control Association (ISACA) for IT management and IT governance, and includes an overview of business continuity and disaster recovery measures.

1.7 Audit Period

Preliminary research, audit planning, meetings, interviews, analysis, testing, review and reporting were carried out during the period January 2022 to August 2022.

1.8 Structure of the Report

This report comprises six Chapters in total, with all but the last Chapter documenting the information collected and highlighting the relevant findings and recommendations. The next five Chapters are structured as follows:

- **Chapter Two** covers the IT management outlook and reviews the management of ICT resources at the AACC.
- **Chapter Three** deals with controls concerning the IT infrastructure and IT operations at the AACC.
- **Chapter Four** includes a review of the principal IT software application, as well as the AACC's website and use of social media.
- **Chapter Five** tackles information security, IT risk management, including business continuity and disaster recovery, as well as security awareness related training at the AACC.
- **Chapter Six** lists the AACC's management comments submitted.

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

1.9 Acknowledgments

The NAO would like to express its appreciation to all the AACC key stakeholders who were involved in this IT audit, namely the Chief Executive Officer (CEO) AACC, ICT Executive AACC, Chief Information Officer (CIO) Information Management Unit (IMU) within the Ministry for Social Policy and Children's Rights (MSPC), and ICT Executives IMU-MSPC, as well as other AACC officers, for the invaluable time and assistance afforded to the NAO's IT audit team throughout this exercise.

The NAO commends the proactive approach and collaborative efforts between the AACC and the IMU-MSPC in modernising their services and undertaking the implementation of a major ICT project, which was evidenced during the audit.

Chapter 2| IT Management

This Chapter covers areas related to IT governance covering strategy and budgeting, procurement and disposal of ICT hardware, asset management and supplier management. Furthermore, the Chapter also reviews ICT support, and the provision of related ICT training to AACC employees.

2.1 IT Strategy and Budgeting

The NAO noted that the AACC does not have a formally documented IT strategy, nonetheless the Entity rigorously abides by relevant Government and MITA Government of Malta ICT (GMICT) policies[12] and guidelines, as well as guidelines issued by the IMU-MSPC. The relationship between the AACC and the IMU-MSPC is defined in greater detail in Section 2.5.

In this regard, the AACC and the IMU-MSPC commented that although the Entity does not have a documented IT Strategic Plan, the AACC continuously plans and coordinates the ongoing IT work programme with the IMU-MSPC. The elements of this work programme are outlined further on in this Section. The IMU-MSPC conduct meetings with the AACC senior management to discuss initiatives in line with the Government ICT Roadmap and Strategies. During these meetings, the ICT business requirements are identified focusing on the specific business area to be automated and the related ICT services and procurement required.

Similarly, in terms of IT budgeting, the NAO was informed that this is tackled during the planning stages of the respective projects, involving substantial background work coordinated by the IMU-MSPC, as well as presentation of budget proposals to obtain the necessary funding for the respective project. The AACC and the IMU-MSPC stated that any requests for IT funding and allocation of human resources is only approved when proper planning has been carried out and benefits emanating from the implementation of the specific projects are identified. This is achieved through continuous discussions between the IMU and the Entity's Management on every ICT project proposal.

In this context, the AACC and the IMU-MSPC pointed out that, the Entity's current major project and key priority is to digitise the AACC operations through the full implementation of the new AACC Case Management System. The implementation of this system is a strategic goal of the AACC, which focuses on the monitoring of the services provided by the Entity against pre-established key performance indicators.

[12] https://mita.gov.mt/portfolio/ict-policy-and-strategy/gmict-policies/

2.2 IT Procurement, Maintenance and Disposal

The NAO was notified that with regards to procedures adopted by the AACC for the procurement, maintenance, repairs, disposal and replacement of IT hardware and equipment, the Entity follows guidelines provided by the IMU-MSPC and MITA policies.

The process for the procurement of IT hardware and equipment, is initiated with the submission of a request for new hardware, which is then authorised by the AACC. Equipment such as desktop computers, laptops, printers, active network equipment (ex. switches, routers, and access points) etc., is procured by the ICT Executive through the centralised MITA procurement process. On the other hand, specialised IT equipment, or any IT equipment not covered by the centralised MITA procurement process, is procured through Requests for Quotations, or through the use of Government's e-Tendering system, following consultation with the IMU-MSPC and MITA.

Meanwhile, maintenance and repairs of IT hardware and equipment is carried out by the third-party hardware suppliers (or their sub-contractors), where a service level agreement is in place. A similar scenario applies for the provision of maintenance and repairs of any equipment which is of a proprietary nature, where the third-party supplier must be contacted directly by the ICT Executive. On the other hand, in cases where the hardware and equipment is neither proprietary, nor covered by a service level agreement, the maintenance and repair services are procured through the Government's e-Tendering system, as indicated above.

With regard to the disposal of IT hardware and equipment, which is obsolete or beyond economical repair, the AACC stated that the disposal process starts once a substantial amount/volume of such items has amassed. A list of equipment, which includes details such as the make, model and serial number of each item, is drawn up by the ICT Executive. An evaluation board is then set up. This board examines the list drawn up, carries out a visual inspection of the related items, compiles the technical description of the items, and proceeds to draft a report with its recommendation for disposal (or otherwise). This is then presented to the CEO AACC, and if approved, this equipment can be disposed of.

Furthermore, the IMU-MSPC stated that a separate procedure is in place, where data storage devices (drives) are removed and separated from the IT equipment, and are securely wiped, before eventually being disposed. When physically disposing of these items, the AACC ICT Executive contacts the approved recycler, and a consignment note is provided by the latter and filed. The audit team was informed that action is then taken to remove the equipment from MITA's Asset Management System (AMS).

This Office was pleased to note that the procedure for disposal of equipment is also covered by a Standard Operating Procedure, although the documented procedure does not make any reference to the secure wiping of data on devices, where applicable. The AACC also remarked that disposal of such equipment is not carried out very often, and the NAO was notified that prior to this IT audit, the last disposal process was carried out in October 2021. A list of the equipment disposed of on this instance was provided to this Office, however, evidence of secure data wiping of the storage devices, on the disposed equipment, and of the consignment note from the recycler, were not made available to the NAO at the time of the audit.

2.3 Asset Management

The NAO noted that in terms of asset management, the AACC's ICT hardware and software inventories are registered on MITA's AMS and MITA's Licence Management System. The AMS database caters for a variety of ICT hardware, including workstations, desktop computers, laptops, whilst the Licence Management System is used to register the core Microsoft software (operating system and software packages) installed on each machine.

The ICT Executive ensures that the above-mentioned inventories are kept up-to-date to reflect the actual ICT assets on AACC's sites (IMU-MSPC is not involved in this process). This enables coordination with other Government Ministries and Entities in terms of transfers and movement of workstations, laptops, etc.

The IMU-MSPC clarified that MITA's AMS was initially intended to record ICT assets, such as workstations, desktops, and laptops. However, the scope of this system was widened to encompass additional ICT equipment, such as monitors, printers, peripherals, auxiliary devices, projectors, etc. (of material value), which were not originally inputted and recorded in this database, although their inclusion is not mandatory.

During its' review of the AACC's inventory records, this Office was pleased to note that the Entity's desktop and laptop computers were appropriately recorded in the AMS, including type, make, model, serial number, inventory number, hardware and software support details, organisation, site, and section or user/s, amongst others. However, details of software installed on the AACC's machines, and relevant licences, were not provided for review.

Meanwhile, details of monitors (such as make, section, user, and inventory number) and printers (make and model, site, office, and inventory number) were also recorded in a separate spreadsheet covering peripherals, although tablets and a projector owned by the AACC were not yet included in this document. Moreover, serial numbers of both monitors and printers were not recorded.

In this regard, the NAO noted that though the inclusion of details of tablets and projectors in the main inventory database, was not yet obligatory, a separate spreadsheet was available for inputting of such details. It was further explained by the IMU-MSPC that the process of including these items in the main database, involves the creation and assignment of new asset codes/tags, along with a review of the whole ICT inventory in its entirety.

2.4 Supplier and Contractor Management

During the course of this audit, the NAO observed that the IMU-MSPC and the AACC maintain a number of ICT related service level agreements or maintenance contracts with the respective third-party vendors or service providers, covering ICT services provided to the AACC.

The principal ICT operations or services covered by such agreements (or by related documentation) included the:

- provision and support of workstations and other IT equipment, as well as use network, Internet, email, VPN, and other key services, provided by MITA;
- the maintenance and support of the CommCare CCG application;
- the procurement and implementation of the new AACC Case Management System; and
- the commissioning, implementation, hosting, maintenance, and support of the AACC website.

The IMU-MSPC clarified that a finalised, formal maintenance and support agreement for the new AACC Case Management System had not yet been drawn up, as the system was not yet fully implemented, although substantial progress had been registered during the course of the audit. As such, the preliminary documentation[13] presented to the NAO for review, covered only certain aspects relevant to maintenance and support, such as service levels and penalties. This documentation did not list key components of a service level agreement, such as the contract period, payment schedule, etc. and the authorised signatories.

In relation to the above, the AACC and the IMU-MSPC also explained that the CCG software application used by the Comm Care Assessment Unit was decommissioned and replaced by a software application module within the new AACC Case Management System. Nonetheless, during its audit testing, the NAO had noted that the CCG software agreement had been signed by all parties and was automatically being renewed for the subsequent year, up to mid-August 2022, prior to this development.

With regard to the AACC website, the NAO was not provided with the respective contract or service level agreement for review.

Further to the above, the NAO was informed that an AACC full-time officer, in the grade of ICT Executive, is directly responsible for coordinating and monitoring the above-mentioned contracts, including, liaising with third-party service providers and IMU-MSPC. With regards to the new AACC Case Management System, the NAO was informed that the ICT Executive is also responsible for managing the related project, whilst the IMU-MSPC is providing assistance in the project implementation. The AACC and the IMU-MSPC held weekly internal meetings to monitor and assess progress, addressed any problems, maintained continuous communication with the AACC senior management and coordinated with the respective third-party supplier/contractor.

[13] Preliminary documentation presented included an Operations Manual documenting operational processes and procedures of the AACC Case Management System, as well as an eProcurement Document outlining the maintenance and support services to be provided by the selected Contractor for the development of the AACC Case Management System.

2.5 IT Team/Unit and IT Support

From the outset of this IT audit assignment, this Office observed that the AACC is supported only by one ICT Executive[14], solely focused and responsible for ICT matters, and who is assisted by a Clerk to handle day-to-day administrative duties. In fact, the NAO noted that the Entity does not have sufficient ICT resources to make up a fully-fledged IT unit/team.

Furthermore, as stated in the first Chapter of this report, the AACC forms part of MFAA. At the time of this audit, the NAO observed that no IMU Office was set up to provide services to this Ministry and its Entities. For this reason, the MFAA continued to make use of the ICT related assistance from the IMU-MSPC, which had supported the AACC when it previously formed part of that Ministry. In this regard, the NAO also observed that the AACC's ICT Executive is fully supported by the CIO IMU-MSPC and his staff. The audit team was informed that the ICT Executive is employed by the AACC and reports directly to the Senior Manager Operations. Nonetheless, in order to fully carry out his duties diligently and efficiently, the Officer does not work in isolation, and also maintains continuous contact with the CIO and the IMU-MSPC.

In terms of support provided, the Officer offers first line of ICT support, which includes desktop support and requests for IT related assistance to all members of staff, at the two main AACC office sites, as well as the various other Residential Homes and Centres. The Officer also fulfilled the role of a Systems Administrator responsible for the management of access rights for AACC users of software applications implemented at the AACC, the monitoring of the AACC Local Area Network (LAN) activity and the allocation of the AACC resources on MITA's hybrid-cloud hosting environment. This ICT Executive was also the key person responsible for ICT Security at AACC and liaison with the IMU-MSPC, MITA and all third-party IT service providers. The Officer was also responsible for IT change management and implementation of ongoing ICT projects within the AACC.

Monitoring and follow up of hardware or software related incidents, and issues with third-party service providers and suppliers, was mostly covered by a service contract between MITA and the IMU-MSPC on behalf of the AACC. In this regard, desktop support was coordinated by MITA. In terms of procedures, the AACC officers experiencing IT related issues or faults were required to personally contact (by phone) MITA Call Centre directly for first line support. Each call was logged by MITA Call Centre on the Agency's IT service management software, MARVAL. Calls falling under the remit of MITA services contract, were handled/solved by MITA support teams. On the other hand, calls which were not within MITA's remit were escalated to the IMU, and forwarded to the AACC's ICT Executive directly to be addressed internally.

[14] Officer promoted to ICT Executive during the course of the IT audit.

2.6 IT Training

The AACC has stated that general ICT training is provided to personnel/employees by the Institute for the Public Services, within the Office of the Prime Minister. Such training is typically provided when it is a requisite for performing duties in certain positions, or upon specific request by the employee and upon approval by the AACC Management.

Furthermore, with reference to the new AACC Case Management System, the AACC remarked that training for this new application was provided through a 'train the trainer' approach. Additional training was provided internally, either by the AACC's ICT Executive, or by the third-party developer/supplier directly. In this regard, the audit team was pleased to note that the IMU-MSPC was very forthcoming in offering and providing its assistance to the AACC's ICT Executive. A list of the training organised can be found in Table two below.

Finally, other than the training provided in respect of the new AACC Case Management System, the AACC stated that documentation indicating general ICT training sessions organised for and attended by its personnel/employees in the past two years was not available.

Service	Training Date
Allied Health	13th January 2021
CommCare/Phlebotomy	24-27th May 2022
Meals on Wheels	23rd June 2022
Dementia Activity Centre	6, 10th July 2022
Telecare Plus	20th July 2022
Centru Servizz Anzjan	10, 21st July 2022
Q&A	3rd August 2022
Carer at Home	11th August 2022
CEO Office	1st September 2022
Finance	7th September 2022
Night Shelter	21st December 2022

Table 2 - Schedule of training sessions

2.7 Observations, Conclusions and Recommendations

IT Strategy and Budgeting

The NAO recommends that a formal IT strategic plan is documented. This should be aligned with the business strategy of the AACC and includes plans of all major IT projects proposed by the AACC/Ministry/IMU.

IT Procurement, Maintenance and Disposal

Whilst this Office was pleased to note that the IT equipment disposal procedure was also covered by a Standard Operating Procedure, however this documented procedure needs to be strengthened to formalise further the data wiping procedure by including such items in particular the formal sign off after the data wiping exercise is successfully completed.

IT Asset Management

The NAO noted that the AACC IT asset details are registered in different systems. In this regard, the NAO suggests that all the above information is stored centrally in one system. The NAO also recommends that details of licences of software applications installed at the AACC is more readily available for future audits.

IT Supplier and Contractor Management

The NAO noted that the contract covering the CCG software was still in operation up to mid-August 2022 although the system was being decommissioned. The NAO recommends that this agreement is reviewed accordingly and if necessary terminated if no longer required.

Furthermore, the NAO recommends that the agreement covering the development of the AACC website is more readily available for future audits.

IT Team/Unit and IT Support

The NAO recommends that the AACC assesses the need for additional IT officers in order to reduce the dependency on a single officer and implement segregation of duties.

The NAO commends the fact that calls are logged on MITA's MARVAL system ensuring that all calls are managed centrally.

IT Training

The NAO recommends that documentation showing recent general ICT training sessions organised for and attended by its personnel/employees is more readily available for future audit purposes.

Chapter 3| IT Infrastructure and Operations

This Chapter details the IT infrastructure setup at AACC, and reviews other key aspects of its IT operations.

3.1 IT Infrastructure (Overview)

The NAO observed that the AACC is connected to the Malta Government Network (MAGNET), which provides connectivity to the Government's Corporate Network and MITA's server related services. These include software application hosting, provision of shared network drives, email and Internet services, and access to the various Government corporate systems.

3.2 Hardware

The equipment listed in Figure three below, as outlined by the AACC themselves, constitutes the hardware in use by AACC:

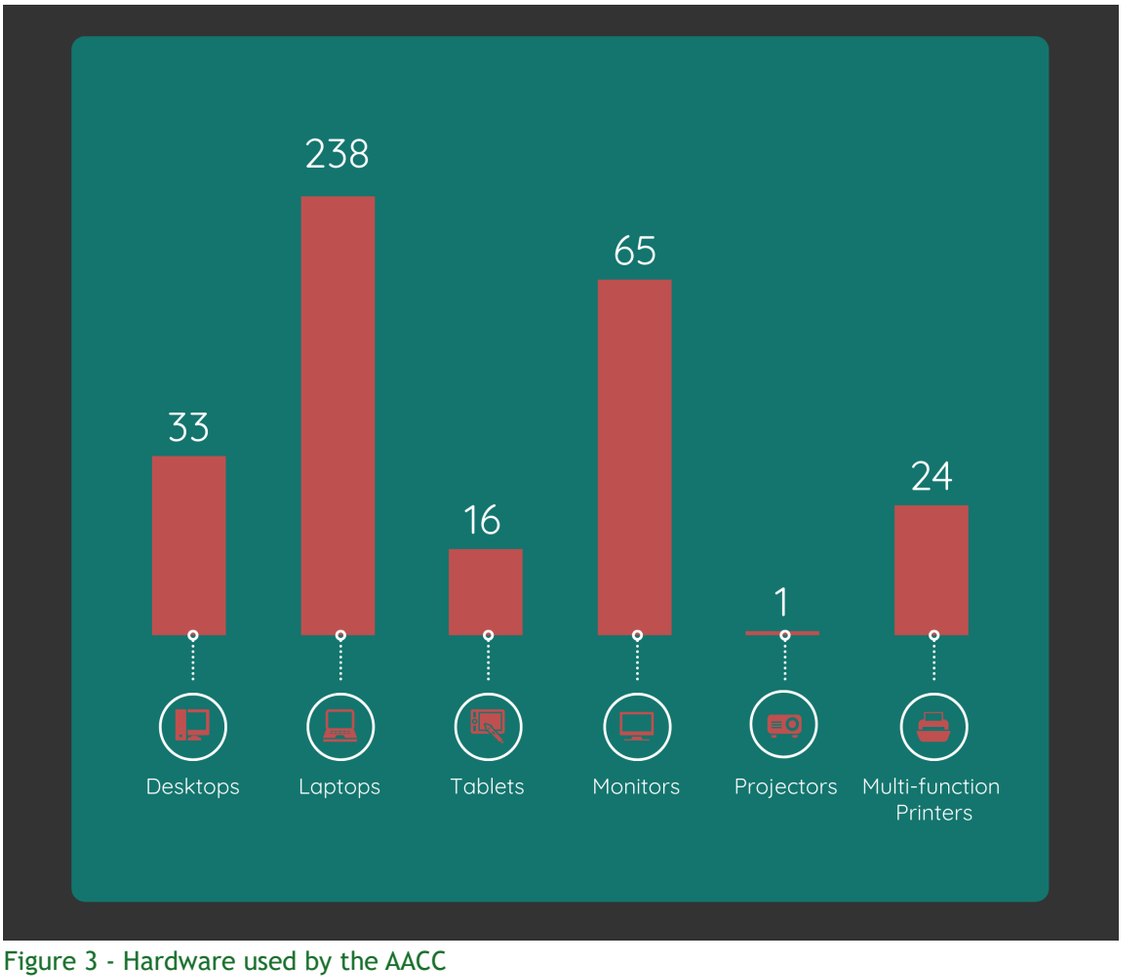


Figure 3 - Hardware used by the AACC

With regard to the above listed hardware, the IMU-MSPC explained that whenever possible, equipment is bought through MITA channels, as already indicated in the previous Chapter. This Office observed that most knowledge workers were provided with laptops, enabling mobility in view of off-site (out of office) duties as well as teleworking requirements. Nevertheless, a few desktops still prevailed. Meanwhile, a number of monitors were mostly utilised as extended displays within the AACC offices. The Entity's offices were also equipped with various multi-function printers. Finally, a small number of tablets were being used by staff performing off-site duties, providing them with online access to the new Case Management System.

3.3 Software

In terms of key software applications in use by the AACC, the NAO observed that at the time of the audit, the AACC was transitioning to its new primary software application, the AACC Case Management System (CMS), although this had not yet been fully developed or implemented, as will be explained further on in the next Chapter. The system is a custom, locally built, software application, which will be used to store, manage, and coordinate data in relation to the majority of services offered by the AACC and its clients. In this regard, the system has already replaced a number of individual legacy systems, spreadsheets and manual processes at the AACC.

Additionally, the AACC also had access to a number of other Government IT systems, namely the Social Policy's SABS Web, Health's CPAS and ICM systems, and Identity Malta's CdB databases, all of which were required directly to process data in order to perform AACC's functions and provide services to its clients.

On an administrative level, the AACC also made use of the DAKAR software system with modules for human resources, leave, and performance appraisals, and the Alcatel Rainbow telephony application enabling online calls over landline for remote users.

The AACC makes use of the Microsoft Office 365 suite on all of its computers, most of which were utilising Microsoft E1[15] licensing model, with the exception of workstations allocated to management, which were using Microsoft E3[16] licensing.

When it comes to operating systems, the NAO noted that, workstations (desktops and laptops) are installed with Microsoft Windows 10, with the image provided by MITA. With regard to the tablet devices, these are running the factory installed, Android 11 operating system with no customisations. In terms of security, these tablets are utilising the built-in security app provided with the device by the vendor.

In terms of software licensing, the NAO noted that the Microsoft Licences are managed centrally by MITA, and covered by the annual services contract entered into between MITA and the IMU-MSPC (as explained in the previous Chapter). The Alcatel Rainbow software licences, are managed by the AACC through the ICT Executive.

[15] Microsoft E1 licensing refers to Microsoft Office 365 software accessed solely through an internet (online) connection.
[16] Microsoft E3 licensing refers to Microsoft Office 365 software installed on the desktop. No internet connection required.

3.4 Servers and Data Storage Equipment

From the early stages of this IT audit, the NAO observed that the AACC is dependent on MITA infrastructure to carry out its functions and provide its services. The Entity also depends on the server backup and recovery services offered by MITA. Additionally, during an on-site review at the AACC's offices, it transpired that the AACC does not possess any server or network attached storage devices given that the AACC's critical data is stored on MITA servers. This setup provides the AACC with a higher level of flexibility, reliability and security in performing its functions.

3.5 Network Cabinets

During on-site visits, the audit team observed that, in terms of equipment, the AACC has three network cabinets installed on premise at its office sites, two at Valletta and one at Qormi.

In this regard, the NAO was pleased to note the presence of individual, dedicated rooms for the placement of the two network cabinets at the Qormi offices. The two rooms housing the network cabinets were strategically placed, one on each floor. During the audit team's visit, it was observed that these were in fact held locked, with the keys to these rooms being kept at the reception desk manned by the security officer, and handed over only to the ICT Executive, being the only authorised officer who can access these rooms, thereby restricting physical access to this essential equipment.

Each of the two rooms were equipped with two adequate air-conditioning (AC) units, providing redundancy in case of an AC unit fault. No additional temperature/humidity monitoring equipment was observed in these rooms. On the positive side, the NAO noted that the room on the second floor was equipped with smoke detectors though none were installed in the other one. The entrance to both rooms from the corridors was monitored by closed-circuit television (CCTV) cameras, whilst adequate fire extinguishers were available in the corridors outside, in the proximity of the entrance to these rooms. The rooms were observed to be relatively clean and well maintained, and the cabinet in one of these rooms was also locked. All patch panels were labelled, however, cable management could be improved. Finally, an uninterrupted power supply (UPS), connected to the network switches in one of the network cabinets, was also observed, providing adequate temporary power in the event of a power outage. The audit team was informed that the UPS was being monitored, albeit in a random manner.

The NAO also noted that the network cabinet at the Valletta offices was housed in a dedicated room, though this small room also contained a number of small cabinets and shelving holding paper documents and various other random items. The room was neither equipped with any AC units, nor any fire detection system, although a dehumidifier was present. Furthermore, during the audit team's on-site visit, it was observed that the door to the room was kept wide open, allowing easy access to anyone.

3.6 Networks (and related services)

As already indicated, the NAO was informed that the AACC's main offices in Qormi and Valletta were connected to MITA's Corporate Domain and the MAGNET, as its primary network connection[17].

This MAGNET connection was used to provide access to all the AACC systems and software applications, and the Entity's services. To provide access to the available services, authorised AACC users connected their workstations to MITA's Corporate Domain through their own unique login credentials. In this regard, devices are configured as per MITA's configured Group Policy Objects[18]. Furthermore, through this network, MITA handles monitoring and control of the network, providing various security controls; such as firewalls, web filtering, malicious code detection and anti-phishing measures, amongst others; as well as regular deployment of various Microsoft updates (which are pushed, downloaded and installed automatically) thereby ensuring that all devices are up-to-date with the latest, essential software updates. In terms of network monitoring tools, the AACC reported that it relies on the SolarWinds software tools utilised by MITA Network Services.

On the other hand, during the course of this IT audit, the audit team also observed that no third-party wireless network connections were available in the above-mentioned office sites. However, a MITA GovMT wireless network connection was available throughout these office sites and is accessible through the users' CORP login.

In the meantime, with regard to network connections within the AACC's Residential Homes and Day Centres, this Office was informed that these connections consisted of:

- MITA/Government connection; and/or
- Third-party service provider connection/s, with a VPN secure connection.

The NAO was informed that third-party connections were more prevalent in Day Centres than Residential Homes.

In this regard, the IMU-MSPC explained that when access to critical medical systems (such as CPAS or ICM) or medical services (such as blood tests, examinations, etc.) was required, the MAGNET connectivity was used.

Meanwhile, for all the remaining non-critical connectivity requirements, such as access to the Internet or email service by the home/residence's administration or staff/users on these sites, the third-party connections, mainly wireless, were used. Nevertheless, a secure VPN connection was used to access the AACC systems or data, over the third-party connections, by authorised users.

---

[17] By way of context, the audit team was also notified that during the period prior to this IT audit, the afore mentioned offices in Valletta were previously connected to the MAGNET via the connection of the overlying Ministry for Finance and Employment offices, but this matter had now been resolved.

[18] Group Policy Objects are a collection of administrative features and settings within Microsoft Windows used by systems administrators to centrally set up, configure, enforce and control the users' working environment on computers attached to a network domain.

3.6.1 Shared Network Drive Server Folders

The NAO observed that the AACC also makes use of MITA's dedicated shared network drive server folders (known as P drive). MITA offers this shared network drive as part of its File Sharing Service packages provided to Government Entities. Authorised AACC users can access and utilise this drive to save and upload their files or folders, or to share files or folders with other authorised AACC users, as per assigned access rights. Data on this drive is backed up by MITA.

3.6.2 File/Folder Access Rights and User Account Management

The NAO observed that since the AACC's workstations were connected to MAGNET and its key systems hosted on MITA's environments, authorised access to network resources was regulated by the related GMICT policies[19].

In addition, the AACC stated that permissions for access to key systems and software applications are assigned to the related CORP user account. In this regard, the NAO was informed that access is granted to users depending on the duties/work involved, and upon specific request and approval by their respective business owner (Manager), who informs the ICT Executive accordingly.

The IMU-MSPC further stated that access to information systems owned by the Ministry for Health requires a signed declaration accepting user's roles and responsibilities.

The NAO was informed that when a user does not require access to the above systems, the respective manager informs the ICT Executive to revoke such licences.

Furthermore, it was explained that whilst the responsibility for authorisation of assignment of file/folder access rights, creation and deletion of user accounts, etc. lies with the AACC, however, the necessary changes are executed by MITA, on the request of the AACC, through an eRFSs procedure raised by the AACC.

With regards to user account login names and passwords, users' passwords were subject to the GMICT Password Policy, with notable password features being adequate in length and complex, expire after a defined period, and history retention with barring reuse of previously used passwords.

3.6.3 Backups and Recovery of Data

Data backup procedures and recovery of data within MITA Corporate Systems (such as SABS, CdB, etc.), the shared network drive (known as P drive), Government email accounts, etc., are all within the MITA remit.

On the other hand, the NAO was notified that the backup of data, with respect to the AACC's primary system (hosted on MITA's environment), lies with the third-party contractor who is developing the system.

[19] https://mita.gov.mt/portfolio/ict-policy-and-strategy/gmict-policies/

3.6.4 Audit Trails

The NAO noted that MITA is responsible for the monitoring and audit logs, for MITA managed solutions, such as the shared network drive (known as P drive), MITA Corporate Systems, etc. These audit trails in relation to AACC users may be provided by MITA upon specific request by AACC Management.

On the other hand, with regard to the AACC's primary system hosted on MITA's environment, since the system was still being developed at the time of the audit, the AACC notified the NAO that there were no instances where access to audit trails was needed.

3.7 Cloud Computing

In response to enquiries made during the course of this audit, the NAO was notified that the AACC utilises MITA's hybrid cloud service, as a hosting platform for its software applications.

The IMU-MSPC indicated that the only exception to the above was the AACC website, which is hosted on a third-party (private) cloud service, managed by the third-party contractor who developed the website, as part of their service level agreement.

Furthermore, the IMU-MPSC indicated that with respect to the AACC's CMS, the software application is hosted on MITA's hybrid cloud service. Access rights to these cloud resources are maintained by the IMU-MSPC and AACC, whereas the environment is managed by the software developer.

Additionally, the NAO was also informed that the previously utilised Community Care Assessments System is also stored on this hybrid cloud service, albeit, in read-only format and for archival purposes only.

The NAO noted that the data stored on this hybrid cloud service included the community services data, emanating from both the new AACC CMS and the previous Community Care Assessments System, as well as other data stored on the AACC's shared network drive (known as P drive). Furthermore, the NAO observed that the offline mailboxes are only stored locally on the workstation and are not being backed up on another drive.

With regards to user data, such as user's personal or shared folders, the AACC stated that users mostly utilise the AACC's shared network drive (known as P drive) for user-related data. Meanwhile, users may also use MITA's Microsoft OneDrive, for personal or shared folders, through MITA's Group Policy Object scripts.

3.8 Internet and Electronic Mail

The NAO noted that the AACC adheres to the applicable GMICT policies related to Internet and email usage as well as web filtering. The AACC added that requests for the whitelisting or blacklisting of a particular URL (or website) that is deemed necessary for work purposes by the AACC, are forwarded to the MITA Call Centre for processing.

The NAO noted that the AACC has 76 generic email accounts. Upon enquiry, the NAO was provided with a detailed list of the above accounts. The AACC stated that the Head/Manager of the unit/section, or an officer appointed by the former, is responsible for the management of such generic email accounts, and access to these accounts is only provided to officers within the same applicable section/unit.

The NAO noted that these generic emails were used to receive and process applications submitted by the general public, thus allowing any user within a given section/unit, to access emails received and proceed with processing these emails accordingly. It was also pointed out that some generic email addresses are used to book AACC rooms for specific meetings with applicants/clients.

An analysis of data provided by the AACC, regarding these generic email accounts and mailboxes as at audit date, revealed two areas which are of concern. This Office observed that a few of these mailboxes had not been used for quite some time, with the last time some of these were used dated back to July 2020, which may indicate that some of these email accounts are no longer required. Additionally, the NAO also noted the current (as at audit date) relatively large size of certain mailboxes, some of which exceed 3Gb and up to almost 7Gb, which may thus warrant some data archiving (where applicable).

3.9 Personal Portable and Mobile Devices

The NAO noted that in regard to the use of personal portable and mobile devices within the AACC's premises, the Entity adopted the Personal Mobile Device Support Policy issued by the former Ministry for Social Justice and Solidarity, the Family and Children's Rights (MSFC) in 2021.

The NAO noted that the AACC has no third-party network connections in its two primary office sites, but only MAGNET and GovMT Wi-Fi connections, thereby automatically subjecting all connecting devices to MITA's standard access and security policies, controls, and monitoring. In this regard, the AACC reported that in the case that a security breach has occurred, the device's owner and user are contacted via email or phone.

3.10 Multi-Function Printers

The NAO noted that the AACC does not have stand-alone printers and the multi-function printers in use were all connected to its internal network and were access controlled. The NAO was informed that secure printing facility was available on these printing devices.

3.11 Observations, Conclusions and Recommendations

Network Cabinets

The NAO recommended that temperature/humidity monitoring equipment is installed in all the network rooms of the AACC offices. Such equipment would control the above-mentioned environmental parameters in real time mode and alert the related officers when the established thresholds are exceeded. Similarly, the NAO recommends that the AACC ensures that all network rooms are equipped with smoke detectors.

Furthermore the NAO recommends that the AACC should ensure that proper cable management and housecleaning is maintained in all network rooms of the AACC offices. This will aid efficient problem identification and resolution as well as reduce fire risks. Additionally, the NAO recommends that the room housing the network cabinet at the Valletta Head office is not used for storage of files/documents, as these could pose a fire hazard, and should be equipped with air-conditioning. Access to the area in question should be controlled and limited to authorised persons only.

Networks (and related services)

The NAO recommends that the AACC ensures that the responsibility for regular backups, related testing of restores and audit trails of the new AACC primary system currently being developed, is clearly defined in the service level agreement, once the new system is fully implemented and commissioned.

Cloud Computing

The NAO suggests that the offline mailboxes of both the AACC users and generic email accounts are backed up on a regular basis so as to ensure that a copy of such offline mail stored locally on workstations is available elsewhere.

Internet and Electronic Mail

The NAO recommends that the AACC conducts an internal exercise to review the need of all current AACC generic email accounts. The NAO noted that some generic email accounts had not been used since July 2020.

The NAO also recommends that the AACC reviews the size of the generic email boxes to be retained and considers the possibility of archiving where applicable, in order to reduce the size of the email box facilitating the backup process.

Personal Portable and Mobile Devices

The NAO recommends that the AACC should draft a fresh policy covering the use of personal mobile devices, based on the former MSFC policy, for the support of personal mobile devices that is currently being used.

Chapter 4| IT Software Applications

The scope of this Chapter is to provide a high-level insight into the key IT application software in use by the AACC, namely, the AACC Case Management System, as well as the AACC's website and the use of social media and networking platforms.

4.1 AACC Case Management System

The AACC Case Management System (CMS) is a case management solution, which records all activities carried out in relation to AACC's clients. This system is part of the Connected e-Government (CONvErGE[20]), which aims to lay down the foundations for further digital transformation across the public service. The CONvErGE project is being delivered through a planned investment of €40 million, of which €28.5 million are derived from EU Funds and the remaining balance from local funds.

The front end is an online web-based application, where clients can apply for multiple services, which they may need or as a trusted agent on behalf of another person. Once the application is submitted, a number of internal processes are triggered simultaneously, in a relational back-end database.

The base client record is common and is accessible by all service areas (units/sections), but each service area can create its own cases pertaining to that client and can record specific service area activities accordingly in a segregated manner.

Additionally, the system is integrated with other Government IT systems, namely, SABS, and CdB databases so that basic client data can be automatically imported from these systems, using specific web services, as and when required.

Given that the AACC is the data owner, any changes or modifications to the system are authorised by the AACC CEO and the ICT support (ICT Executive), in liaison with the IMU-MSPC. In this context, it was explained that the IMU-MSPC is an integral and strategic part of the process of developing and introducing the new AACC CMS, and consequently regular weekly meetings are held between both parties.

The AACC CMS software application is based on Microsoft SQL server and is a dedicated, customised solution intended for the specific needs of the AACC. The system's front end is an online web-based application built on K2 Workflow. The software is being developed and implemented by a local third-party developer. The system is hosted on MITA's hybrid cloud environment. In this context, it was also clarified that MITA is responsible for the provision of its application hosting services related to this system whilst the AACC ICT Executive is responsible for administering the system in terms of user account management.

[20] https://www.eipa.eu/epsa/connected-egovernment-converge/

In terms of access management, the audit team observed that access to the AACC CMS application is restricted to authorised users only, via user login and password. In this regard, the AACC confirmed that access to this application is obtained through the user's Government's CORP account, and consequently, governed by the Government Password Authentication System. This implies that if a user is already connected to the MAGNET, via the CORP credentials, the user will just need to access the system's URL link (website) to access the system automatically, logging in with the same credentials (single sign on). On the other hand, if the user is not connected to the CORP Domain (such as a remote working user), apart from having to use the CORP credentials, MITA's mandated multi-factor authentication is required to access the system.

The above implies that the policies related to CORP Domain password, in terms of password complexity, password expiry, password history and blocking access after successive unsuccessful attempts to input incorrect credentials, are also applicable to this system. Furthermore, given that the AACC users' workstations have been imaged and configured to MITA's policies as indicated earlier on, it should be noted that login credentials have to be re-inputted by the user to access the system after a specific amount of idle time, as this machine would have automatically logged off the user for security purposes.

The NAO noted that as at audit date, there were circa 377 users having access to this system. In terms of access levels, these can be categorised into Normal users, having access to individual modules, and the Systems Administrator, having access to all modules. Meanwhile, the Super Administrator role is currently assigned by the IMU-MSPC to the system developer, having full access rights to manage the system until this is fully developed, implemented and eventually consigned to the AACC. This role will then be assigned, either to the AACC directly or the IMU-MSPC.

With regards to users' access level and access rights assigned to users, the NAO was informed that these are specifically allocated according to each specific module that a user will use to carry out his/her duties (as opposed to have the same rights across all modules used by the user), and according to the user's position/grade. User access rights are assigned by the ICT Executive, upon an email request from the unit Manager/Head, with the latter being solely responsible for approving which access rights are to be given or revoked for each user in his/her team.

Further to the above, users who are on temporary leave (such as maternity leave, etc.), have their access rights either disabled or revoked, by the ICT Executive, usually as per instructions given by the module/unit Manager/Head. The IMU-MSPC also clarified that over and above that, MITA's setup automatically disables access to CORP accounts, which have not been used for a specific period of time, barring them from accessing the system. In the meantime, users who have been transferred, have had their employment terminated, have resigned or retired, will all have access rights removed by the ICT Executive, after being informed/instructed via email by the Unit Manager/Head as indicated above.

In this regard, pursuant to enquires made during the course of this IT audit, this Office was pleased to note that an internal exercise had been carried out where a number of users, who were no longer engaged by the AACC, were completely removed from the system. An updated list of users was then compiled by the AACC Human Resources and sent to the ICT Executive. The AACC further stated that it plans to

carry out this procedure on a regular basis going forward, using the Staff Adjustment Report, listing all employee movements and absences/leaves, prepared by the AACC Human Resources.

Given that the system is still under development, the AACC does not have Super Administrator rights, hence cannot access audit trails directly unless provided by the developer. The AACC stated that, as at audit date, the audit trails had never been requested.

However, the IMU-MSPC and the AACC provided this Office with a number of snapshots, some of which were extracted from the system back-end database using database query tools, indicating a number of ways (or processes) which can be executed and by which administrators may access and verify the audit trail of a transaction or other changes done through the system. At a high level, the snapshots provided included, using the K2 Workflow's reporting functionality, which provides a history of how the case has moved and transitioned through the Workflow system, indicating, for example, the number of process (case) instances started, whether these are still active, have expired or have been completed, and the originator. The system also has a Process Instance Data Audit function with a Data Audit Log, which looks at individual processes (cases) and provides values that were passed to the workflow system. On a more detailed level, another snapshot provided a log of every change to the case data. The history of these changes were maintained through the Case lifetime. The related table includes details such as Case ID, Action ID, Created by (user), Action Started and Action Ended (date and time stamp).

The final two detailed audit snapshots provided, utilised Microsoft SQL Server Management Studio to run a specific SQL query. This can be used to access the SQL Change Data Capture audit feature enabled on key tables within the system database, and thus extracts a list of every change done to the data in that table (where a new copy of the record is stored for every change made to the data in that table). This included details such as Case ID, User ID, Date and Time. It can also be used to access the K2 Workflow's internal audit tables to view case history, case changes done through forms, case logins, etc., with various details.

In terms of system integration with CDR and SABS web, the NAO was informed that this is essential since the AACC CMS automatically retrieves basic client details (record) from the CDR database using the client's ID number. Subsequently, the same client ID number is used to automatically verify whether or not the applicant is registered as having a Health Pink Card or not, thereby saving the applicant, and the AACC, from verifying this information manually.

The NAO noted that during the course of this audit, there were no known pending bugs which had yet to be fixed. It was also clarified that, at this stage, when the system is still being developed, typically, users will identify bugs when the system is not working as expected and inform the ICT Executive accordingly. The latter will carry out the necessary testing to verify and confirm the validity of such bugs. Once confirmed, the ICT Executive will then log a call to inform the developer so as to rectify the issue. The developer will then check and follow up accordingly.

In this context, the IMU-MSPC further clarified that incident criticality is relevant, depending on the relevance of the module and the AACC service effected by the issue, thus noting that this criticality will determine the priority given to the incident when it is logged. Overall, the NAO was informed that

at this stage, the AACC and the IMU-MSPC are satisfied with the feedback and support being provided by the developer in terms of bug fixes and incident resolution, adding that whenever they had critical issues (during development), the developer took the necessary steps to mitigate the arising issues in a timely manner.

In the meantime, the NAO was informed that this system is envisaged to provide the AACC with all the required functionality, including anything that was provided by legacy systems to date, and encompass all services provided by the Entity. The IMU-MSPC indicated that post full implementation, there should be no pending legacy systems left in operation.

In this context, it was outlined by the IMU-MSPC that the implementation of the new system required the import of all relevant data from existing databases, and spreadsheets, to the new system. When this process is fully completed, the AACC users would not need to resort to the legacy systems.

The IMU-MSPC evaluated any remaining possible dependencies on Excel spreadsheets or the legacy system/s, with the aim to fully integrate and automate the whole process through a number of enhancements to the new system. The project team looked at each module and assessed what enhancements were required for it. The NAO was also informed by the AACC that enhancements which had been requested as at audit date covered services such as Home Help and Telephone assessments, Handyman service, Carer at Home, and Meals on Wheels, amongst others.

The IMU-MSPC stated that fortnightly meetings are held with the AACC CEO where the project team discusses the program of works, what has been achieved, what still needs to be implemented, etc.

The NAO was informed that the IMU-MSPC is currently monitoring the level of availability/performance of the new system. It is envisaged that the system redundancy may have to be strengthened and increased considering the anticipated usage of over 600 users from within the AACC with circa 20 modules.

The audit team was informed that in terms of software documentation, the contractor is to provide the IMU-MSPC with the final source code and related documentation, when the project is finally completed and the system is delivered/handed over, as per tender agreement. This can then be kept, updated and maintained with a schema of any changes made.

With regards to user manuals, the audit team was provided with a copy of the system's Core Module User Training document. The AACC claimed, that while the document is primarily used for user training purposes, it also serves as a user manual, outlining the main functionalities of the core modules. The audit team was also informed that any user having access to the system and core modules will have access to this document. In this regard, this Office was pleased to note that this document is rather detailed, with various screenshots and detailed descriptions with step-by-step instructions.

The NAO was also informed that the users were provided with on-the-job training, and dedicated one-to-one sessions where deemed necessary, so as to familiarise themselves with the new system and its functionality. The AACC added that initially, training courses had been provided online, during the

COVID-19 pandemic, and in view of difficulties encountered by some users, these were followed up with additional in-person training for some of the units.

The audit team observed that in terms of reporting functionality, each module within the AACC CMS features its own specific reporting facilities. Each of these reporting facilities includes monthly and annual reports and ad-hoc reports from the respective Managers. The IMU-MSPC added that at this stage, other reports may still be required.

4.2 AACC Website

The NAO reviewed the AACC website *https://activeageing.gov.mt* and noted that it included information about the various services offered by the Entity, as well as links to downloadable application forms.

Broken links within the website were found when selecting:

- The link to the downloadable copies of the AACC organogram within the "Dwarna" page.
- The link to the downloadable copy of the "National Strategic Policy for Active Aging: Malta 2014 – 2020" within the English version of the landing page.
- The link to the downloadable form for "Dementia Care at Home" and link to further information within the same page.
- Selecting the "Iktar Dwarna" button within the "Dwarna" page.

A missing link was found to the downloadable privacy policy document in the "Terms of Use" page.

The link to the "Apply Online" button for Support for Dementia brings up the Spanish version of the page by default instead of the English version.

4.3 Social Media

The NAO noted that the AACC have their own Facebook page *https://www.facebook.com/ActiveAgeingandcommunitycare/*, which was found to be very informative and regularly updated. The Facebook page had 4,018 likes with 4,293 followers at the time of this audit. This page included various news updates on related events using text, visuals and video recordings.

The NAO noted that closer monitoring of comments/reviews is required so that any irrelevant reviews, which may mislead the public, are reported to Facebook.

4.4 Observations, Conclusions and Recommendations

AACC Case Management System

The NAO recommends that the AACC ensures that the roles and responsibilities associated with system administration/operations and backup/restore processes are clearly defined in the related service level agreements to be signed once the new AACC CMS system is fully commissioned. Furthermore, the NAO recommends that the AACC needs to ensure that all future backups need to be stored off-site in an adequate secure place.

The NAO recommends that the AACC holds discussions with the IMU MSPC, as well as the software developer, to make any system/infrastructural adjustments that may be required, to ensure continuous availability and adequate performance levels when the system is working at full load i.e. being accessed by circa 600 AACC users across the various services that the Entity offers.

AACC Website

The NAO recommends that a review of the AACC website is carried out to ensure that all broken and missing links are restored. This needs to be followed up with a periodic website review to ensure that the web content remains updated.

Chapter 5| Information Security and IT Risk Management

This Chapter takes a look at information security controls and IT security measures adopted by the AACC, to maintain integrity, confidentiality and availability of data. Furthermore, this Chapter also looks at the management of IT risks within the AACC, to identify, assess and prioritise potential risks, so as to draw up related recommendations to mitigate or reduce such risks.

5.1 Anti-Virus and Anti-Malware

As detailed earlier on in Chapter Two, given that the AACC depends on MITA for server and network infrastructure services, and is joined to MITA's Corporate Domain through MAGNET, the AACC benefits from MITA's security setup covering the above services. For example, all the AACC workstations are configured using MITA's Microsoft Windows image, whilst subsequently MITA manages the prevention and spread of malware in its various forms, through anti-virus definitions and malware threat protection updates, which are pushed automatically over its network to all workstations joined to its (Government) Domain.

5.2 Business Continuity and Disaster Recovery

Enquiries made by the NAO revealed that the AACC has neither conducted a Business Impact Analysis (BIA) nor a risk assessment exercise as at audit date. In addition, it also transpired that the AACC does not have a Business Continuity Plan (BCP) or a Disaster Recovery Plan (DRP).

The AACC also asserted that no particular incidents of non-availability of primary IT systems, which might have impacted its overall operations, had been recorded to date.

In this regard, the AACC reiterated that the Entity's critical data is all stored on MITA's servers, thus implying that the applicable risks are rather curtailed. The AACC also added that the request for services processes currently in place, can revert back to a manual, paper-based, process in the event of a major disaster occurring.

Further to the above, the NAO also confirmed that the AACC does not have any alternative, disaster recovery site from where the Entity could resume its principal operations in the event of a disaster. Nonetheless, the AACC reported that in such a scenario, if a major disaster had to occur and impact its main office site at Qormi, the Entity may opt to use its offices in Valletta (Ċentru Servizz Anzjan) as the core premises for customer care and other front end customer facing purposes, whilst allowing other officers to work remotely, as had been done during the COVID-19 pandemic.

5.3 Information Classification

The NAO was informed that the AACC does not have an Information Classification policy of its own. Given the nature of data captured by the AACC, in processing the applications submitted by the public for the various services offered by the Entity, the NAO cannot stress enough the importance of information classification and data retention. An Information Classification policy would ensure awareness of the type of data being handled.

Information Classification consists of the categorisation of data to ensure that all the officers within the Entity treat classified data in a similar way. Data classification is the basis for protecting the confidentiality of data and minimising the risks of mishandling data, including unauthorised destruction, modification or disclosure, which could lead to legal repercussions.

5.4 Data Retention

The Data Protection Act specifically states that the "Data controller shall ensure that personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed."

The NAO noted that this policy[21] is available on the AACC website.

5.5 IT Security Awareness Training

The NAO was informed that the AACC's officers regularly receive informative emails through MITA's Security Aware's mailing list, which regularly informs Government users of present IT security threats making them aware of and how to avoid becoming a victim to such threats. However, the NAO was not provided with evidence showing the attendance to IT security related courses by the AACC staff.

5.6 Physical Access Controls

During the audit visits to the AACC's premises, the NAO reviewed the physical access security measures and controls in place on site at the AACC's offices in Qormi and Valletta.

In this context, this Office was pleased to note that security measures at the AACC Head office in Qormi included a combination of access card reader, a CCTV (video surveillance) system, an intruder alarm, a visitors' logbook and the presence of an on-site third-party security officer/guard. The NAO is concerned with the limited physical access measures in place at the AACC's offices in Valletta (Ċentru Servizz Anzjan).

[21] https://activeageing.gov.mt/wp-content/uploads/2021/04/DP-Retention-Policy-EN.pdf

5.6.1 Access Card Reader and Intruder Alarm

The NAO observed that an access card reader was installed at its Head office in Qormi during the audit team's on-site visit. In the meantime, the AACC indicated that an intruder alarm was installed at its Residential Care Home in Mellieħa.

5.6.2 Video Surveillance System

The NAO also observed that a CCTV is installed at its Head office in Qormi, during the on-site visit. This system comprises a total of 21 cameras.

Furthermore, the AACC confirmed that a CCTV system was also installed at its Mellieħa and Mtarfa Residential Care Homes, as well as its Dementia Centre at Safi.

In terms of security cameras installed at these sites, the NAO was informed that these systems comprise 16 cameras at Mellieħa residential home and two cameras at Mtarfa residential home. No data was provided by the AACC on the number of cameras installed at the remaining AACC sites.

This Office was also informed that the video surveillance system retains footage for a period of five days, before it is automatically overwritten. The NAO noted that the AACC have a CCTV policy documenting the details of the data controller and the right of access however the AACC did not provide details of the internal procedure to be followed to access such footage.

5.6.3 Visitor Logging, Visitor IDs and Visitors' Policy

As part of the audit testing carried out during the course of this audit, the IT audit team also reviewed controls in place related to visitors at the AACC's offices. During the on-site visits, it was observed that a visitors' logbook/register was being maintained by the AACC. In terms of procedure, the NAO was informed that pursuant to signing the visitors' logbook/register provided by the security officers at the reception, the latter is to provide visitors with a temporary Visitors' ID. The security officer is then instructed to either phone the person needed to come meet the visitor at the reception area, or to escort the visitor to the respective officer. The NAO noted that the procedures in place ascertain control over visitors, whilst maintaining a record for audit purposes.

Notwithstanding the above, the NAO gathered that the AACC does not currently have a formally documented visitors' policy in place.

5.6.4 Security Guard

As stated above, the AACC's Head office in Qormi made use of the services of a security guard. Furthermore, the AACC pointed out that the services of a security guard is also used at four of its Residential Care Homes, located at Mellieħa, Mtarfa, Mosta, Floriana; its Dementia Centres at Safi and Mtarfa, as well as at Dar Padova in Għajnsielem, Gozo.

5.7 Fire Detection and Fire Suppression Systems

Whilst carrying out the on-site reviews at the AACC's premises, the NAO observed the fire detection controls and fire suppression measures at the AACC's offices in Qormi and Valletta.

As already mentioned earlier on, the NAO noted the presence of smoke detectors at the AACC's Qormi offices. The NAO also observed that a fire alarm system was installed at the AACC's Head office in Qormi. Moreover, the Entity notified this Office that similar fire alarm systems were installed at most of its other sites, namely: its four Residential Care Home at Mellieħa, Mtarfa, Mosta, and Floriana; five of its Day Centres at Mellieħa, Żurrieq, Żejtun, Birżebbuġia, and Bormla and its Safi Dementia Centre. The NAO was also informed that the fire alarm system at Dar Padova in Għajnsielem, Gozo was in the process of being procured at the time of audit testing.

With regard to fire suppression measures, the IT audit team observed the prevalence of fire extinguishers installed on both levels of the building housing the AACC's offices in Qormi. The AACC stated that in total there were 35 units on premise, whilst confirming the three types of fire extinguishers installed, being Dry Powder (ABC) (14 units), Carbon Dioxide (CO2) (13 units), and Foam (8 units). These fire extinguishers were duly inspected and serviced regularly by the respective third-party contractor on a yearly basis, with the last inspection carried out in the last quarter of 2021. Finally, the NAO was pleased to note that a listing of all the fire extinguishers on site, including their type and location, is maintained by the AACC and was provided for IT audit purposes.

5.8 Observations, Conclusions and Recommendations

Anti-Virus and Anti-Malware

Given that the new AACC CMS system is hosted on MITA's infrastructure, any service level agreements with both the system developer and MITA should clearly outline their responsibilities with respect to the upkeep of anti-malware and anti-virus protection at a server level.

Business Continuity and Disaster Recovery

The NAO recommends that the AACC conducts a BIA in order to identify the risks to be mitigated through a Business Continuity and Disaster Recovery Plan. The following paragraphs outline the details of the BIA, BCP and DRP processes.

Business Impact Analysis

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

The NAO recommends that the AACC lists and reviews its critical and non-critical functions, and from each critical function determine:

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

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

Once the above process is completed, the AACC should then determine its recovery requirements. This will identify the business and technical requirements to recover each system or critical function in the event of an interruption, including disasters, and to provide guidance based on which detailed recovery procedure is to be adopted. Furthermore, the NAO recommends that the AACC should identify threats to the assets related to the above critical functions and assess the level of vulnerability to those threats. Fires, floods, acts of terrorism/sabotage, hardware/software failures, virus attacks, DoS attacks, Cybercrimes and internal exploits are all examples of the type of threats that are to be analysed, assigning a probability assessment value to each. The NAO recommends that the AACC identifies preventive measures that will reduce the possibility of these threats occurring, and to identify countermeasures to successfully deal with these threats, if and when they develop.

Business Continuity and Disaster Recovery Plans

The primary objective of a BCP is to protect the AACC in the event that all or parts of its operations and/or Information Systems are rendered unusable, and to help the entity recover from the effects of such events. The BCP defines the roles and responsibilities and identifies the critical IT application programs, operating systems, networks personnel, facilities, data files, hardware and time frames required to assure high availability and system reliability based on the inputs received from the Business Impact Analysis exercise.

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

Once the DRP is concluded, the plan should be tested regularly. Moreover, the key persons should familiarise themselves with the recovery process and the procedures to be followed in the event that the DRP is invoked.

Information Classification

The NAO recommends that the AACC drafts its own Information Classification policy. This policy should define security levels for data based on the sensitivity, value and criticality of the data. The policy shall:

- List the principles that need to be followed to protect data (depending on the security level assigned to it).
- Stipulate the manner through which one can disclose data (depending on the security level assigned to it).
- List the people/Entities to whom this data may be disclosed to (depending on the security level assigned to it).
- List the procedures to be followed when disposing of data (depending on the security level assigned to it).

IT Security Awareness Training

The NAO recommends that the AACC reviews the IT security courses available at the Institute for the Public Services in collaboration with the MSPC CIO's office. Furthermore, the NAO suggests that such training should be provided on a regular basis and should form part of the induction training programme for all newly recruited staff at the Entity.

Physical Access Controls

The NAO recommends that the AACC reviews the physical access controls present in all its premises, including the residential homes and day care centres, in order to ensure the current measures are adequate and updated with the use of current technology.

Fire Detection and Fire Suppression Systems

The NAO recommends that the AACC carries out a regular review of the fire detection and suppression systems in all of the Entity's sites so as to ensure full adequate coverage in all sites at all times.

Chapter 6| Management Comments

The final Chapter of this report presents the comments given by the AACC senior management.

6.1 AACC Management Comments

Key Findings and Recommendations

Following the background information on the AACC and overall structure of this report, provided in Chapter One, the following Chapter covers areas related to ICT governance, support, and training.

The following are the key findings and recommendations included in **Chapter Two**:

- *Whilst acknowledging the considerable efforts being undertaken by the AACC in the area of IT management and development, notwithstanding the need of additional resources in this important area, the NAO noted that the ACCC does not yet have a formal IT strategic plan and recommended that such a plan is drafted, which would include plans of all major IT projects proposed by the AACC/ Ministry/IMU.*

  As correctly pointed out, the AACC shall work on drafting an IT Strategic Plan including the core Information System.

- *Though the NAO was pleased to note the AACC's procedure for IT equipment disposal, this Office made some recommendations to formalise further the data wiping process forming part of the procedure.*

  The disposal SOP was shared by the MSPC IMU as the AACC apply the same procedure. Note has been taken and further information will be reviewed by the MSPC.

- *Given that one of the AACC's key software applications (CCG system) is in the process of being replaced, the NAO recommended that the AACC ensures that the related service agreement is terminated once the system is no longer in use. With regards to the agreement related to the AACC website, the Office recommended that the document is more readily available for audit purposes.*

  The CCG Agreement has been terminated and solution no longer in use. It is set to read-only and plans for decommissioning are to be considered.

  As for sharing of agreements, we deem these were provided as requested.

- *The NAO noted the urgent need for additional IT officers in order to reduce the dependency on one official and ensure proper segregation of duties. Otherwise, timely implementation of all our recommendations would be extremely difficult, if not outright impossible.*

  Correctly highlighted and in agreement. The AACC need to invest in additional human resource in IT. Since the time of such audit, the MFAA had appointed a new Chief Information Officer (CIO – Mr. Daniel Mangani) who shall be consolidating resources under his capacity and administer accordingly.

Chapter Three *of the report covers the IT infrastructure setup at the AACC, and reviews other key aspects of its IT operations. The following are the key findings and recommendations:*

- *In view of security issues, the NAO noted the lack of temperature and humidity monitoring equipment in the network rooms at the AACC offices in Valletta and Qormi and recommended that such equipment is installed. Furthermore, this Office recommended that the AACC ensures that all its network rooms are equipped with smoke detectors as some did not have such devices. The NAO also recommended that the AACC should ensure that proper cable management and housecleaning is maintained in all network rooms of the AACC Valletta and Qormi offices. With reference to the network cabinet in the Valletta office, the NAO recommends that the area is equipped with air-conditioning, cleared of stored files/documents in the vicinity and has its physical access limited to authorised staff only.*

  Recently works were conducted at the AACC Valletta to the data cabinet and LAN infrastructure. Point has been noted and in agreement to recondition/organisation of server rooms/data cabinets and equip with proper facilities management.

- *The NAO recommends that the AACC ensures that the responsibility for regular backups, related testing of restores and audit trails of the new AACC primary system currently being developed, are clearly defined in the service agreement once the new system is fully implemented and commissioned.*

  This shall be clearly defined upon complete handover of the project from the Supplier to the AACC. Moreover, the AACC IT has requested supplier for a redundancy proposal for business continuity purposes. Awaiting reply from Supplier.

- *With reference to the offline mailboxes of both the AACC user and generic email accounts are backed up on a regular basis, as recommended by the NAO. The use of certain generic email accounts should be reviewed as some were last used in July 2020. The AACC should also consider the option of archiving in order to reduce the size of some of the generic mailboxes.*

  With reference to mailboxes clean-up exercise, we believe that this in an important check that should be followed every quarterly to ensure resources both operational and financial aspects are kept up-to-date.

Chapter Four *includes a review of the AACC Case Management System, as well as the Entity's website and social media. The key findings and recommendations included in this Chapter, included amongst others the following:*

- *With reference to the new AACC CMS system being implemented, the NAO recommended that the AACC ensures that:*

    - *Roles and responsibilities associated with system administration/operations and backup/ restore processes are to be clearly defined in the related services agreement to be signed once the new AACC CMS system is fully commissioned.*

      Drafting of SOP by the AACC/Supplier should be presented upon completion of the project with regards to the operational, maintenance and support depict the role and responsibilities of each respective party.

    - *Future backups are stored off-site in an adequate secure place*

      As for backups, it is being tackled the same as point two of Chapter Three.

    - *Meetings with the IMU-MSPC and the software developer are held to discuss system/ infrastructural adjustments that maybe required to ensure continuous availability and adequate performance levels when the system is working at full load (i.e. being accessed by circa 600 AACC users across the various services that the Entity offers).*

      Important to note that the AACC/MSPC IMU/Supplier hold Bi-Weekly meetings to address and monitor strategically the implementation progress. As well monthly meetings are held to address/monitor operational issues between the AACC/Supplier.

- *The NAO recommended that the AACC takes the necessary steps to ensure that all broken and missing links within the AACC website are restored. A periodic website review to ensure that the web content remains updated, was also recommended by this Office.*

  With reference to outdated website content and links, such exercise is an ongoing endeavour between the IT and AACC officers. Online updates are carried out daily as part of the operations.

Chapter Five *of this report looks at the IT/IS Security and IT related risk management at the AACC. The following are the key findings and recommendations:*

- *With regards to measures to protect from software viruses and malware, the NAO recommended that any service agreement covering the support and hosting of the new AACC CMS system should clearly outline the responsibilities for anti-malware and anti-virus protection at a server level.*

  Security measures are important to be adhered. Whilst servers are hosted at MITA and monitored, it is still the responsibility of the client to ensure proper security measures are in place. The AACC IT shall follow-up with Supplier/MITA to check that respective software agents are configured.

- *The NAO recommended that the AACC conducts an IT business impact analysis in order to draft the related Business Continuity and Recovery Plans which the Entity did not have.*

  Agreed, an IT Business Continuity Plan and Recovery Plan are essential and to be considered and part of the AACC CMS system.

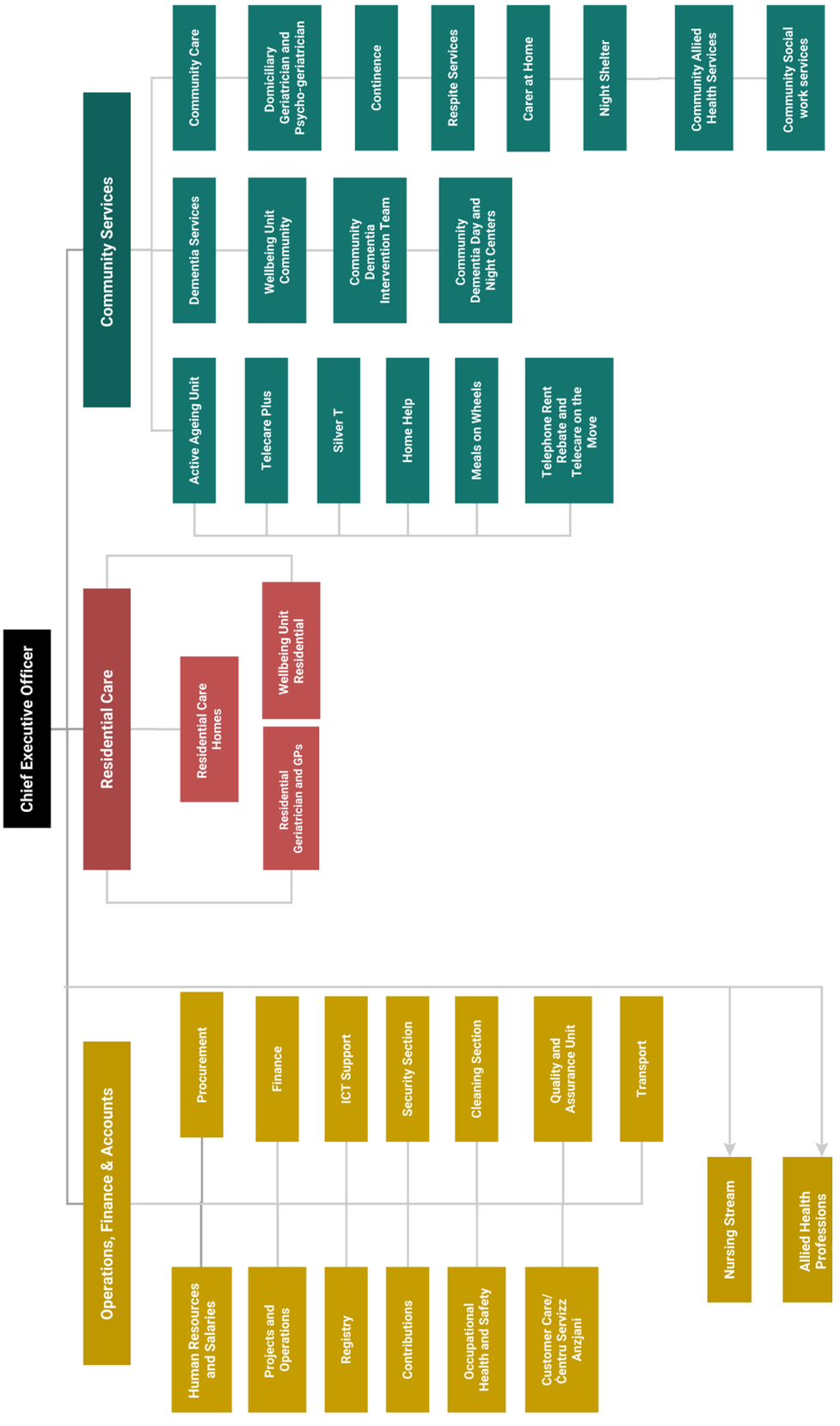
- *It was observed that the AACC did not have an information classification policy, which defines the security levels for data based on data sensitivity, value and criticality. The NAO therefore recommended that the AACC should draft such a policy. The NAO also recommended that the AACC drafts its data retention policy and follows the Government's current HR retention policy with respect to the Entity's HR data.*

  Agreed, an Information Classification Policy is essential and to be considered.

- *The NAO recommends that the AACC reviews the physical access controls present in all its premises including the residential homes and day care centres in order to ensure the current measures are adequate and updated with the use of current technology. Furthermore, this Office also recommended that the AACC carries out regular reviews of the fire detection and suppression systems in all of the Entity's sites.*

  The AACC shall coordinate with personnel responsible for Facilities Management to ensure proper checks and maintenance are carried out, including assessment to physical site security at residential homes/day care centres.

Annex A| AACC Organigram



2022 Reports issued by NAO

NAO Annual Report and Financial Statements

July 2022	National Audit Office Annual Report and Financial Statements 2021

NAO Audit Reports

May 2022	Performance Audit: Assisting Individuals with Dementia and their Caregivers within the Community
May 2022	Joint Report on Management of Plastic Waste in Europe
May 2022	Ministry for Finance and Employment: An Analysis on Revenue Collection Financial Year 2020
June 2022	An evaluation of performance audits in the public sector: Common audit findings (2017–2020)
June 2022	Follow-up Audits Report by the National Audit Office Volume I 2022
July 2022	Performance Audit: Procuring the Public Transportation Service
October 2022	The COVID-19 pandemic - Business continuity within the public administration
October 2022	Performance Audit: A Follow-up on the 2018 Strategic Overview of Mount Carmel Hospital
November 2022	Follow-up Audits Report by the National Audit Office Volume II 2022
November 2022	Report by the Auditor General on the workings of Local Government for the year 2021
November 2022	Performance Audit: Care for the Elderly in Gozo
December 2022	IT Audit: Online Census 2021
December 2022	Report by the Auditor General on the Public Accounts 2021