the gpaa

Department:
Government Pensions Administration Agency
REPUBLIC OF SOUTH AFRICA

| YOUR BENEFITS our responsibility |

GPAA Enterprise Architecture
For The
Modernisation Programme

Version 1.35

December 2023

Document Classification:

Confidential

Document Versions

Version	Revision Date	Prepared / Revised by	Business Unit	Comments
V1.0	September 2023	Dumisani Zinondo	ICT	First Final Version
V1.10	September 2023	Dumisani Zinondo	ICT	Revised Final Version after peer review.
V1.20	September 2023	Dumisani Zinondo	ICT	Added Business Processes section and updates based on Final peer review 29/09/2023.
V1.30	October 2023	Dumisani Zinondo	ICT	Added Migration section as a separate chapter and created separate sections for system, data and integration migration considerations. Updates to Integration Architecture and Application inventory.
V1.35	December 2023	Dumisani Zinondo	ICT	Expanded on the ICT Security Framework components.

Approval/Adoption of Document

Pule Moiloa

Digitally signed by Pule Moiloa
Date: 2023.12.18 13:16:07 +02'00'

PULE MOILOA

MODERNISATION PROGRAMME MANAGER

DATE:

Support/ [redacted]

Meiring Coetzee

Digitally signed by Meiring Coetzee
Date: 2023.12.19 14:54:40 +02'00'

MEIRING COETZEE

CHIEF INFORMATION OFFICER

DATE:

Support/ ~~Not Supported~~

Paul Masipa

Digitally signed by Paul Masipa
Date: 2024.02.09 11:59:27 +02'00'

PAUL MASIPA

GEPF ICT MANAGER

DATE:

Recommended / ~~Not recommended~~

ESTI DE WITT
Digitally signed by ESTI DE WITT
Date: 2024.12.12 11:06:33 +02'00'

ESTI DE WITT

CHIEF DIRECTOR LEGAL/MODERNISATION STEERING COMMITTEE CHAIRPERSON

DATE:

Recommended / Not recommended

KEDIBONE MADIEHE

CHIEF EXECUTIVE OFFICER / MODERNISATION PROGRAMME OWNER

DATE:

Approved / Not Approved

MUSA MABESA

GEPF PRINCIPAL EXECUTIVE OFFICER / MODERNISATION PROGRAMME SPONSOR

DATE:

Table of Contents

References

The table below provides a list of reference documents that are applicable to this document. These are mainly acts, laws, frameworks and standards.

Ref.	Title	Publisher	Version/Date
[R1]	GEP Law & Rules		
[R2]	GPAA Strategic Plan 2020/2021 – 2024/2025	GPAA	
[R3]	GPAA ICT Strategy	GPAA	
[R4]	GPAA Modernisation Business Case - PAS	GPAA	
[R5]	GPAA Modernisation Business Case - CRM	GPAA	

[R6]	GPAA Modernisation Business Case - FMS	GPAA	
[R7]	GPAA Capability Model	GPAA	
[R8]	GPAA Modernisation Business Requirements - PAS	GPAA	
[R9]	GPAA Modernisation Business Requirements - CRM	GPAA	
[R10]	GPAA Modernisation Business Requirements - FMS	GPAA	
[R11]	GPAA Enterprise Architecture	GPAA	
[R12]	GPAA Information Security Strategy	GPAA	

Table 1: Reference Documents

These documents may be seen as an extension of this document.

Ref.	Title	Publisher	Version/Date

Table 2: Applicable Documents

1 Introduction

1.1 Executive Summary

The GPAA, has historically maintained an operation supported by legacy systems and processes that, while effective, have started to show signs of age in the era of digital transformation. The GPAA requires an urgent shift towards a modern infrastructure.

The purpose of this Enterprise Architecture (EA) document is to outline the technology guidelines for this Modernisation Program, aiming to deliver a more responsive, transparent, efficient, and digitally evolved GPAA.

The EA aims to support the vision to transform GPAA into a digitally-forward, citizen-centric agency that offers seamless, efficient, and transparent pension administration services, anchored by robust, flexible, and secure IT architecture.

The document aims to assess the existing EA practice withing GPAA and develop a roadmap to an improved EA practice while also assisting the Modernisation Programme with EA requirements to review and update existing Business, ICT, and cross cutting Information Security Architectures. The work is aimed at developing a robust and comprehensive request for proposal for the replacement of the legacy pension administration system, CIVPEN which is made up of three key modules for replacement i.e., Pension Administration System, Financial Management System and Customer Relationship Management.

Key Architecture Objectives:

1. **Digitisation of Services:** Enhance user experience by providing online platforms for pensioners to view, manage, and engage with their pension accounts.
2. **Data Integration & Analytics:** Establish a unified data repository with analytics capabilities to enable data-driven decision-making and predictive analytics.
3. **Infrastructure Modernization:** Transition from legacy systems to cloud-based platforms to ensure scalability, resilience, and efficient service delivery.
4. **Cybersecurity Enhancement:** Strengthen the security posture of GPAA, ensuring the privacy and safety of pensioner data.
5. **Process Optimization:** Streamline and automate pension administration processes to enhance efficiency and reduce manual interventions.
6. **Stakeholder Collaboration:** Foster a collaborative environment with internal and external stakeholders to ensure a holistic approach to modernization.

1.2 Scope Of Work

The GPAA is looking to meet the requirements of the Modernisation Programme through Enterprise Architecture development / refresh to render the following:

- Define and develop the EA that represents a blueprint of GPAA providing a common understanding of the organization.
- Depict GPAA as a business broken down into business units, which have certain capabilities.
- Unpack capabilities through enabling series of value streams that require information.
- Document the Organization, Capability, Value Streams, and Information foundation.
- Define business processes, functions and models that are relevant to the achievement of the Modernisation Programme and the Digitalisation of the GPAA.
- Develop the new or revised Business Operation Model
- Revisit the enabling ICT Architecture components covered by the domains for Data/Information Architecture, Applications, Architecture, Technology Architecture, and the underlying Information Security Architecture.
- Liaise with GPAA internal and external stakeholders
- Manage the change control process for each of the solutions implemented under Modernisation Programme.
- Implement, monitor, evaluate and improve the EA performance.

Maintain all EA documentation and models according to GPAA approved EA Tool and repository.

1.2.1 Deliverables

Based on the Scope of Work above, the following Deliverable Components shall be required in this document.

The following deliverables have been defined on:

Business Architecture

- Business & Operating Model Canvas
- Organizational Model
- Capability Model & Value Streams
- Documentation
- Business Process Architecture
- Target Operating Model
- Business Architecture – Strategic Alignment
- Process Change Management
- Compilation, Consolidation & Publishing

ICT Architecture

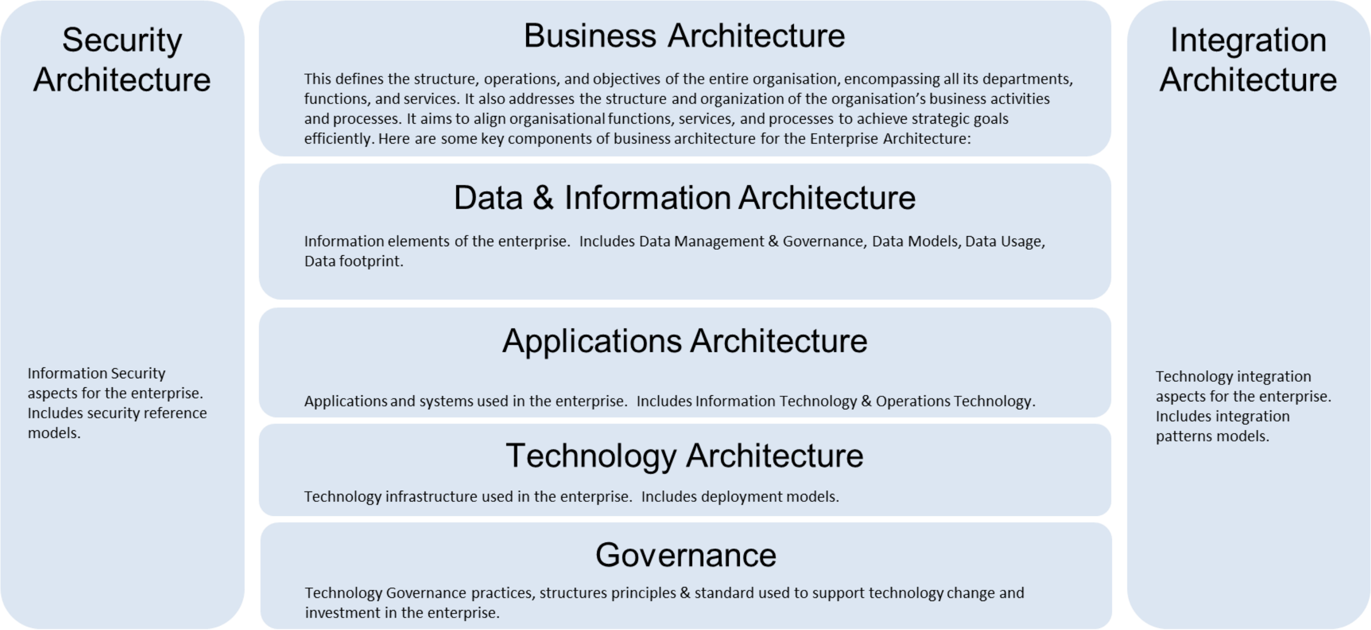
AS-IS & TO-BE ICT Architecture

- Business Architecture
- Data Architecture
- Applications Architecture
- Integration Architecture
- Infrastructure Architecture
- Security Architecture

2 Enterprise Architecture

The Enterprise Architecture (EA) is a strategic planning framework that aligns an organization's business goals with its information technology strategy. It allows Organisations to organize, standardize, and coordinate their IT infrastructure to meet business objectives.

The key components of EA are shown below and shall be defined as domains in the rest of this document.



Security Architecture

Information Security aspects for the enterprise. Includes security reference models.

Business Architecture

This defines the structure, operations, and objectives of the entire organisation, encompassing all its departments, functions, and services. It also addresses the structure and organization of the organisation's business activities and processes. It aims to align organisational functions, services, and processes to achieve strategic goals efficiently. Here are some key components of business architecture for the Enterprise Architecture:

Data & Information Architecture

Information elements of the enterprise. Includes Data Management & Governance, Data Models, Data Usage, Data footprint.

Applications Architecture

Applications and systems used in the enterprise. Includes Information Technology & Operations Technology.

Technology Architecture

Technology infrastructure used in the enterprise. Includes deployment models.

Governance

Technology Governance practices, structures principles & standard used to support technology change and investment in the enterprise.

Integration Architecture

Technology integration aspects for the enterprise. Includes integration patterns models.

Figure 1: Enterprise Architecture Overview & Focus Areas

2.1 Enterprise Architecture Principles

Enterprise Architecture (EA) principles are general rules and guidelines that guide an organization's IT strategy, aligning it with business goals. They aim to support decision-making, standardize technology, and allow a strategic approach to the scalable growth of IT systems.

The GPAA Architecture principles are used to guide the creation of architecture at GPAA.

These architecture principles are largely influenced by the architecture principles provided by TOGAF.

Refer to Appendix A for a list of principles used for business, data, applications, and technology architectures.

3 Business Architecture

Business Architecture Overview

Business architecture generally serves as a blueprint for an organization, aligning the business's strategy with its objectives, structure, and operations. It allows the organization to clearly understand how various parts interconnect, helping in informed decision-making, promoting efficiency, enhancing agility, and supporting innovation and customer focus.

Below is a brief overview of its purpose:

- **Strategic Alignment**: It ensures that the day-to-day operations align with the organization's strategic goals, thereby facilitating coherent decision-making.
- **Improves Efficiency**: By providing a clear view of organizational structure, processes, information, and technology, business architecture helps in identifying and eliminating redundancies, promoting more efficient resource allocation.
- **Enhances Agility**: By providing a holistic view of the business, it allows for quick responses to changing market conditions, regulatory changes, or innovations in technology.
- **Facilitates Communication**: It serves as a common language or framework that different parts of the business can refer to, enabling better collaboration and understanding between various functions and levels of the organization.
- **Risk Management**: Identifying and mapping dependencies and interrelationships within the organization enables better risk management and can prevent potential issues from arising.
- **Supports Innovation**: By understanding how different parts of the business interact and work together, Organisations can identify opportunities for innovation and growth.
- **Customer Focus**: Understanding and mapping the customer journey and experience can help in aligning products, services, and internal processes to meet and exceed customer needs and expectations.

The Business Architecture for the Government Pension Administration Agency (GPAA) would also aid in supporting the efficient management, organization, and execution of the agency's operations.

The business architecture defined includes the following areas:

- Business strategy, business goals
- Business capabilities
- Value streams
- Information Mapping
- Organisation structure
- Business processes

3.1.1 Strategic Overview

The Government Pensions Administration Agency (GPAA) is a government component which reports to the Minister of Finance and administers funds and schemes on behalf of the Government Employees Pension Fund (GEPF), National Treasury and other smaller funds.

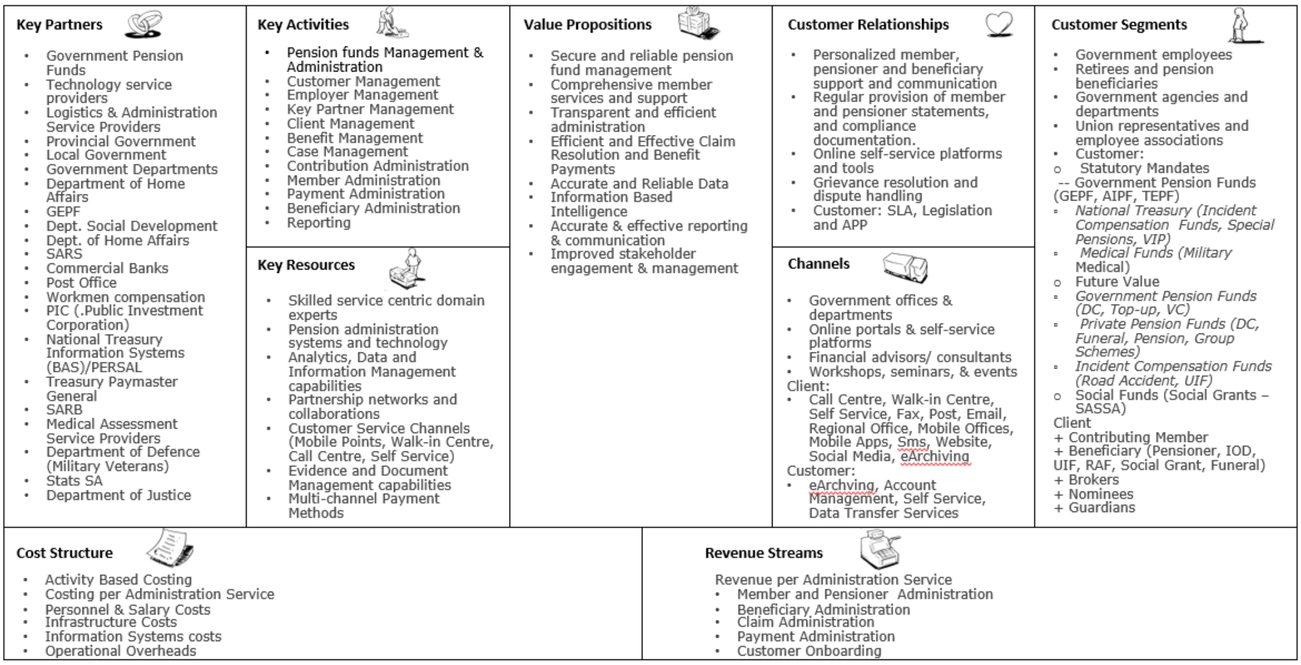
The GPAA has formulated seven strategic outcomes which will guide its programmes for the next 5 years.

- Optimal core support
- Capable and reliable administration system
- Digitised processes
- Efficient admission management
- Efficient contribution management
- Efficient case management
- Reduced payment turnaround time

3.1.2 Business Model Canvas

The GPAA's model revolves around efficient management of pension funds and related benefits for government employees. The emphasis is on transparent, compliant, and sustainable practices that ensure the financial well-being of retirees and other beneficiaries. Engagement with both governmental and financial entities is crucial to the GPAA's success, as is maintaining the trust and satisfaction of its members through reliable and accessible services. Given its public nature, the GPAA must also place a strong focus on ethical considerations, social responsibility, and alignment with broader governmental policies and goals.

GPAA is responsible for managing, administering, and overseeing pension funds for government employees and, in some cases, other citizens. The Business Canvas Model for GPAA outlines the key components that enable it to provide services.



Key Partners

- Government Pension Funds
- Technology service providers
- Logistics & Administration Service Providers
- Provincial Government
- Local Government
- Government Departments
- Department of Home Affairs
- GEPF
- Dept. Social Development
- Dept. of Home Affairs
- SARS
- Commercial Banks
- Post Office
- Workmen compensation
- PIC (.Public Investment Corporation)
- National Treasury Information Systems (BAS)/PERSAL
- Treasury Paymaster General
- SARB
- Medical Assessment Service Providers
- Department of Defence (Military Veterans)
- Stats SA
- Department of Justice

Key Activities

- Pension funds Management & Administration
- Customer Management
- Employer Management
- Key Partner Management
- Client Management
- Benefit Management
- Case Management
- Contribution Administration
- Member Administration
- Payment Administration
- Beneficiary Administration
- Reporting

Key Resources

- Skilled service centric domain experts
- Pension administration systems and technology
- Analytics, Data and Information Management capabilities
- Partnership networks and collaborations
- Customer Service Channels (Mobile Points, Walk-in Centre, Call Centre, Self Service)
- Evidence and Document Management capabilities
- Multi-channel Payment Methods

Value Propositions

- Secure and reliable pension fund management
- Comprehensive member services and support
- Transparent and efficient administration
- Efficient and Effective Claim Resolution and Benefit Payments
- Accurate and Reliable Data
- Information Based Intelligence
- Accurate & effective reporting & communication
- Improved stakeholder engagement & management

Customer Relationships

- Personalized member, pensioner and beneficiary support and communication
- Regular provision of member and pensioner statements, and compliance documentation.
- Online self-service platforms and tools
- Grievance resolution and dispute handling
- Customer: SLA, Legislation and APP

Channels

- Government offices & departments
- Online portals & self-service platforms
- Financial advisors/ consultants
- Workshops, seminars, & events

Client:

- Call Centre, Walk-in Centre, Self Service, Fax, Post, Email, Regional Office, Mobile Offices, Mobile Apps, Sms, Website, Social Media, eArchiving

Customer:

- eArchving, Account Management, Self Service, Data Transfer Services

Customer Segments

- Government employees
- Retirees and pension beneficiaries
- Government agencies and departments
- Union representatives and employee associations
- Customer:

○ Statutory Mandates

-- Government Pension Funds (GEPF, AIPF, TEPF)

▫ *National Treasury (Incident Compensation Funds, Special Pensions, VIP)*

▫ *Medical Funds (Military* Medical)

○ Future Value

▫ *Government Pension Funds (DC, Top-up, VC)*

▫ *Private Pension Funds (DC, Funeral, Pension, Group Schemes)*

▫ *Incident Compensation Funds (Road Accident, UIF)*

○ Social Funds (Social Grants – SASSA)

Client
+ Contributing Member
+ Beneficiary (Pensioner, IOD, UIF, RAF, Social Grant, Funeral)
+ Brokers
+ Nominees
+ Guardians

Cost Structure

- Activity Based Costing
- Costing per Administration Service
- Personnel & Salary Costs
- Infrastructure Costs
- Information Systems costs
- Operational Overheads

Revenue Streams

Revenue per Administration Service

- Member and Pensioner Administration
- Beneficiary Administration
- Claim Administration
- Payment Administration
- Customer Onboarding

Figure 2: GPAA Business Model Canvas

The Government Pension Administration Agency (GPAA) is a South African public service organization responsible for administering pensions and related benefits for government employees. It plays a vital role in ensuring that pensions are correctly administered, distributed, and maintained.

The business model is confined within governmental regulation, collaboration, and public service provision. It's essential to recognize that the GPAA operates with the government's overarching social and economic objectives in mind, rather than working to generate profits. The focus is on sustainability, security, and compliance with regulations, and the business model would be shaped to facilitate these requirements efficiently and effectively.

The business canvas and model for the GPAA incorporates the following:

Key Partnerships

Partners may include various government departments, financial institutions, auditors, and regulatory bodies to ensure compliance with laws and financial security.

These generally include the following:

- South African government departments and entities
- Pension fund trustees
- Financial institutions and banks for the disbursement of pensions

Key Activities

The primary activities include collecting contributions, administrating funds, processing and paying benefits, ensuring compliance with regulations, and providing customer support.

These generally include the following:

- Member record and contribution administration
- Administering pension funds
- Processing pension claims
- Keeping track of contributions from government employees
- Ensuring compliance with legal and financial regulations

Key Resources

These include skilled employees, legal frameworks, technology, governmental support, and financial management tools that ensure accurate administration of pensions.

These also include the following:

- IT infrastructure for pension processing and tracking
- Skilled personnel for managing funds, related benefits and financial analysis
- Legal teams for ensuring legal, commercial and compliance, together with other teams
- Physical offices and facilities

Value Propositions

The GPAA's primary value comes from its administration services as pertains benefits, contributions, membership.

These also include the following:

- Support for Pension Fund Managers and related Customers
- Reliable and consistent administration of pension funds and related benefits for government employees and beneficiaries
- Efficient processing and payout of pensions and related benefits.

Customer Segments

Customers:

These are organisations on whose behalf the Administrator (GPAA) administers its benefits.

Clients

These are generally contributing members and beneficiaries of the fund.

These also include the following:

- Current government employees contributing to the pension fund
- Beneficiaries of non-contributory funds and related benefits
- Retired government employees receiving pensions
- Beneficiaries of deceased government employees

Customer Relationships

GPAA deals directly with the Government Funds and Entities (as Customers) and is expected to build relationships with its customers through transparent communication, accessibility, and dedicated customer service based on the administration mandate and agreed service levels.

These also include the following:

- Administrative support to Customers, for engagement/cases on government employees regarding their pension queries
- Regular communication and updates about pension status and changes
- Dispute resolution mechanisms for pension-related issues

Channels

The GPAA provides services through online portals, offices, and call centres.
These also include the following:

- Physical offices throughout the country

- Online portals and systems for pension management and queries
- Call centres and helplines for pension-related assistance

The list of channels shall continue to grow based on opportunities.

Cost Structure

The main costs would stem from staff salaries, technology and system maintenance, administrative expenses, and compliance costs.

These also include the following:

- Operational costs of running offices and facilities
- IT maintenance and upgrade costs
- Salaries and benefits for employees
- Miscellaneous administrative expenses

Revenue Streams

As a government agency, the GPAA's revenue is not based on profit generation but rather comes from government funding. The funding ensures that the organization can fulfil its mandate to administer pensions effectively.
The GPAA its "revenues" come from Government allocations and funding.

There is opportunity to revise this model and create an efficient and sustainable operating model. This will be managed and executed in the relevant initiatives and forums outside the Modernisation Programme.

Overall Strategy and Model

The business model for GPAA focuses on administrative services for the associated Clients and Customers, and their members (including beneficiaries).

The model requires close coordination with various government bodies and financial institutions and continuous engagement with the stakeholders.

3.1.3 The GPAA’s value chain

The GPAA’s core processes, specifically benefits administration which includes client administration, contributions and maintenance, pensioner maintenance and benefits processing, rest on the pillars of support services. These comprise of Corporate Services, Financial

Management, Business Enablement (ICT), Strategic Support and Governance. Currently core processes and support services are improved and enhanced to achieve the GPAA's strategic outcomes.

The GPAA's value chain is depicted in the Figure below:

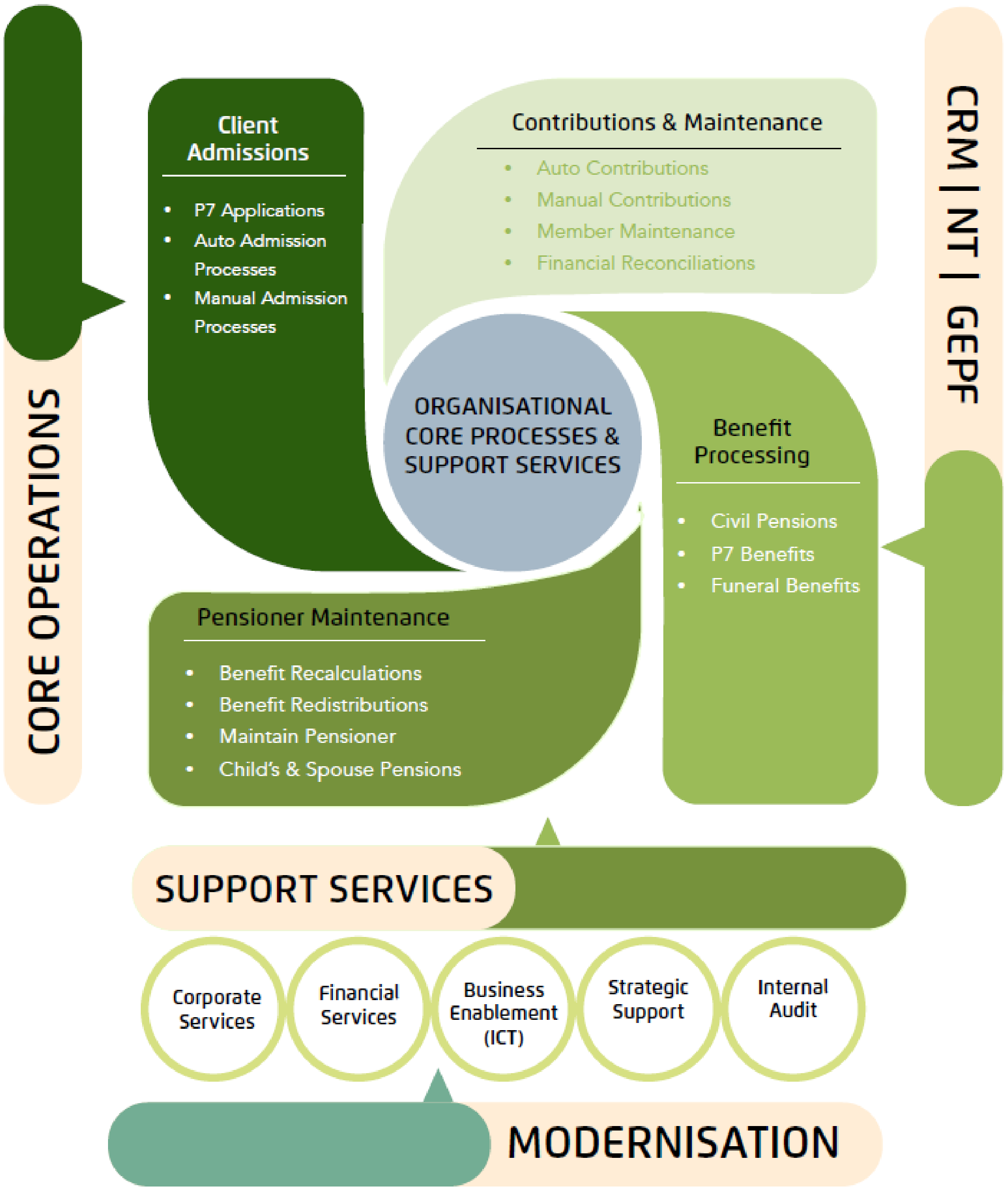
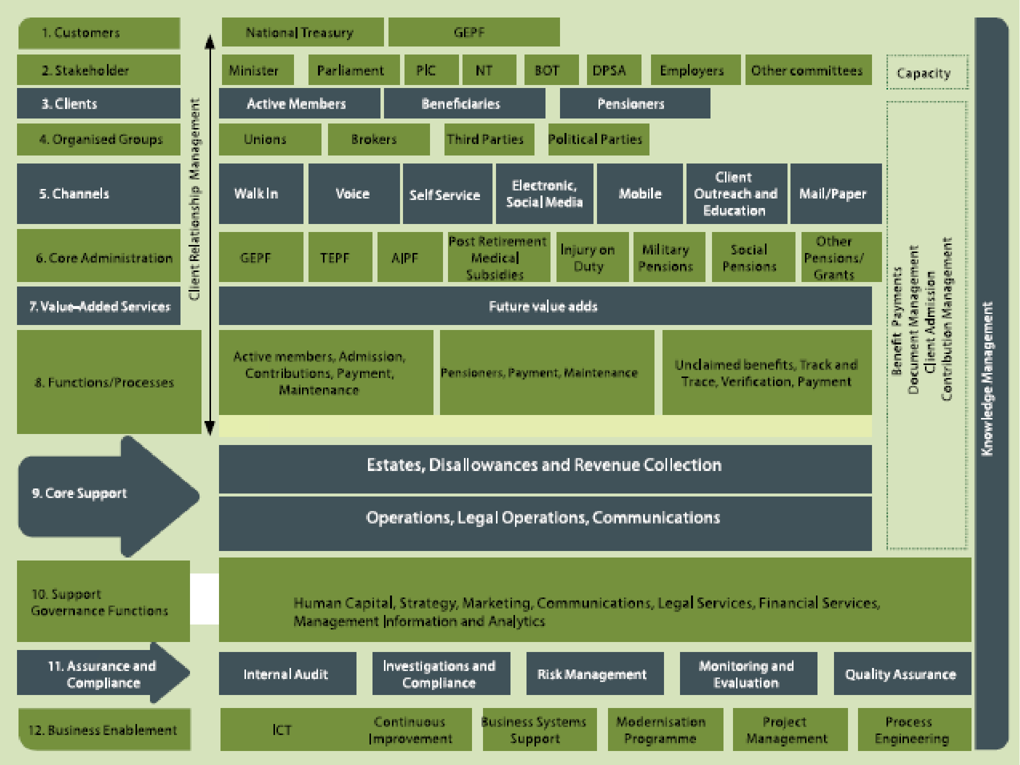


Figure 3: GPAA Value Chain

The GPAA's Capability Model responds to the twelve (12) performance areas within which the core processes, stakeholders and functional areas resides. The model compliments the GPAA's structure, processes and capabilities as depicted in the figure below:



1. Customers: National Treasury | GEPF

2. Stakeholder: Minister | Parliament | PIC | NT | BOT | DPSA | Employers | Other committees

3. Clients: Active Members | Beneficiaries | Pensioners

4. Organised Groups: Unions | Brokers | Third Parties | Political Parties

5. Channels: Walk In | Voice | Self Service | Electronic, Social Media | Mobile | Client Outreach and Education | Mail/Paper

6. Core Administration: GEPF | TEPF | AIPF | Post Retirement Medical Subsidies | Injury on Duty | Military Pensions | Social Pensions | Other Pensions/ Grants

7. Value-Added Services: Future value adds

8. Functions/Processes: Active members, Admission, Contributions, Payment, Maintenance | Pensioners, Payment, Maintenance | Unclaimed benefits, Track and Trace, Verification, Payment

9. Core Support: Estates, Disallowances and Revenue Collection | Operations, Legal Operations, Communications

10. Support Governance Functions: Human Capital, Strategy, Marketing, Communications, Legal Services, Financial Services, Management Information and Analytics

11. Assurance and Compliance: Internal Audit | Investigations and Compliance | Risk Management | Monitoring and Evaluation | Quality Assurance

12. Business Enablement: ICT | Continuous Improvement | Business Systems Support | Modernisation Programme | Project Management | Process Engineering

Figure 4: GPAA's structure, processes and capabilities consolidated summary view

3.1.4 **Business Services**

The GPAA's key Business Services represent the service offering that the organisation offers to its customers, clients, stakeholders and partners. The following are some of the key services that form part of the Business Model Canvas.

Pension Funds Administration	Customer Management	Employer Management	Key Partner Management
Client Management	Benefit Management	Case Management	Contribution Administration
Member Administration	Payment Administration	Beneficiary Administration	Reporting

GPAA aims to provide services to ensure efficient handling of the agreed mandate.

The services offered encompass a wide range of functions that require efficient coordination, adherence to legal requirements, robust financial management, and effective communication with various stakeholders.

Below is a description of the services listed:

Service	**Pension Funds Administration**
Description	This entails the operational administrative handling of the pension scheme, including enrolment, compliance with legal requirements, record-keeping, and the distribution of information to members and relevant parties.
Activities	• Overseeing the operational framework for government pension funds. • Regulating and managing pension fund investments to ensure optimal returns. • Implementing policies and best practices as prescribed by regulatory authorities. • Ensuring compliance with applicable pension laws and regulations. • Oversight of pension funds to ensure compliance with regulatory requirements. • Processing and reconciliation of contributions and benefits. • Maintenance of pension fund records, including member details and transaction histories.

Service	**Customer (i.e. Pension Fund Managers) Management**
Description	This includes coordination, communication, and relationship management with Pension Fund Managers, providing them with necessary data, support, and collaboration to ensure the proper execution of investment strategies.
Activities	• Facilitating reporting and communication channels between the agency and fund managers. • Organizing regular meetings to assess the progress and direction of the funds. • Engagement with Pension Fund Managers, understanding their needs, and providing tailored services. • Offering training and support. • Facilitating communication and information exchange.

Service	**Employer Management**
Description	This deals with the coordination and communication with the employers who contribute to the pension funds. It includes managing employer contributions, compliance checks, and handling employer-related inquiries.
Activities	• Coordinating with government departments or agencies to ensure timely and accurate pension contributions. • Educating employers on their obligations regarding pension contributions. • Handling discrepancies or errors in employer contributions. • Liaising with government employers to manage pension contributions. • Providing support for employer-related inquiries and compliance issues.

Service	**Key Partner Management**
Description	This involves the management of relationships with various stakeholders and partners such as banks, regulatory bodies, and others involved in the ecosystem.
Activities	• Collaborating with financial institutions, regulatory bodies, and other stakeholders to ensure smooth fund management. • Negotiating and finalizing agreements and contracts with service providers. • Managing relationships with third-party vendors, and technology providers. • Ensuring alignment with regulations and standards.

Service	**Client Management**
Description	This includes managing relationships with the individual contributors and beneficiaries of the pension fund, handling queries, complaints, and requests, and ensuring a satisfactory customer experience.
Activities	• Assisting pensioners and potential pensioners with inquiries, grievances, or requests.

	• Implementing a responsive customer service channel, including helplines, chatbots, and email support. • Providing regular updates to customers regarding pension policies or changes.

Service	**Benefit Administration**
Description	This covers the calculation, review, approval, and distribution of pension benefits, including early retirements, disability pensions, and survivor benefits.
Activities	• Overseeing the calculation and disbursement of pension benefits to eligible retirees. • Managing the various pension benefit schemes available to retirees. • Ensuring timely processing and approval of pension claims.

Service	**Case Management**
Description	Managing individual cases regarding disputes, appeals, and special circumstances, ensuring that they are handled efficiently and in accordance with laws and regulations.
Activities	• Handling individual cases of disputes, grievances, or special circumstances. • Collaborating with legal teams for cases that require judicial intervention. • Ensuring all cases are documented, tracked, and resolved in a timely manner.

Service	**Contribution Administration**
Description	This involves the handling of contributions from both employees and employers, including calculation, collection, reconciliation, and ensuring proper allocation to individual accounts.
Activities	• Tracking and verifying contributions made by employers and employees. • Reconciling discrepancies in contribution amounts.

Service	**Member Administration**
Description	Managing the records and details of all members in the pension fund, including enrolling new members, maintaining up-to-date records, and overseeing the status changes such as retirement, termination, or death.
Activities	• Maintaining up-to-date records of all active and retired members. • Assisting members with changes in personal details or circumstances. • Managing the onboarding and exit processes for members.

Service	**Payment Administration**
Description	Overseeing the accurate and timely distribution of pension payments to retirees and beneficiaries, including handling tax withholdings and other deductions.
Activities	• Overseeing the disbursement of pension payouts. • Ensuring timely and accurate payments to all beneficiaries. • Reconciling payment issues or discrepancies.

Service	**Beneficiary Administration**
Description	Management of beneficiary information and ensuring proper distribution of benefits in cases such as death or disability of a pension fund member.
Activities	• Maintenance of beneficiary information. • Managing and updating records of nominated beneficiaries for each member. • Facilitating the transfer of funds to beneficiaries upon a member's demise. • Providing support and guidance to beneficiaries during the claim process. • Coordination of benefit payments to beneficiaries.

Service	**Reporting**
Description	Producing regular reports on various aspects of pension and benefits administration, compliance, member statistics, and other key metrics. These reports may be provided to regulators, internal management, Pension Fund Managers, and other stakeholders.
Activities	• Generating periodic reports on fund performance, contributions, disbursements, and other relevant metrics. • Facilitating audits and regulatory checks by providing necessary data. • Offering customized reports to government entities, partners, or other stakeholders as required.

3.1.5 Service Model

The GPAA provides administration services to its Customers, GEPF, National Treasury and other smaller funds, for Pension Funds and various Benefits. The diagram below provides some context on this service model, showing that the fund, schemes, benefits, members, pensioners, recipients, clients and beneficiaries are not directly managed by the GPAA but by its customers.

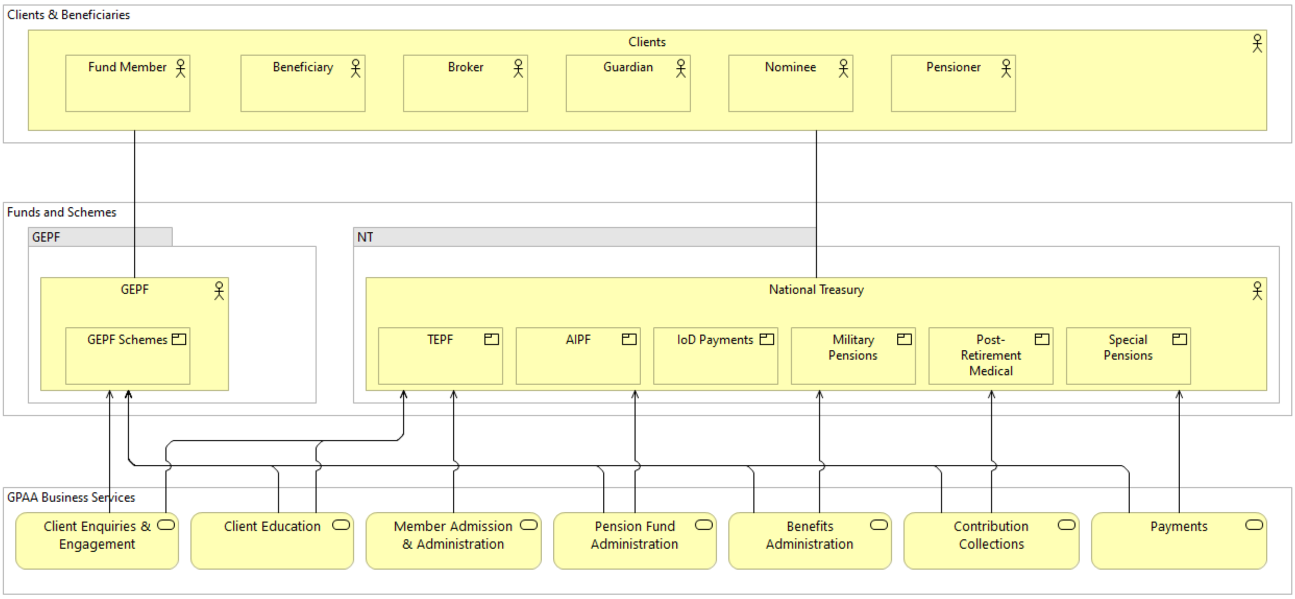


Figure 5 : GPAA service model

3.1.6 **Organisation View**

The GPAA Organizational View breaks down the core business into its integral business units and departments.

Current Structure: The current and outgoing organizational view is shown below.

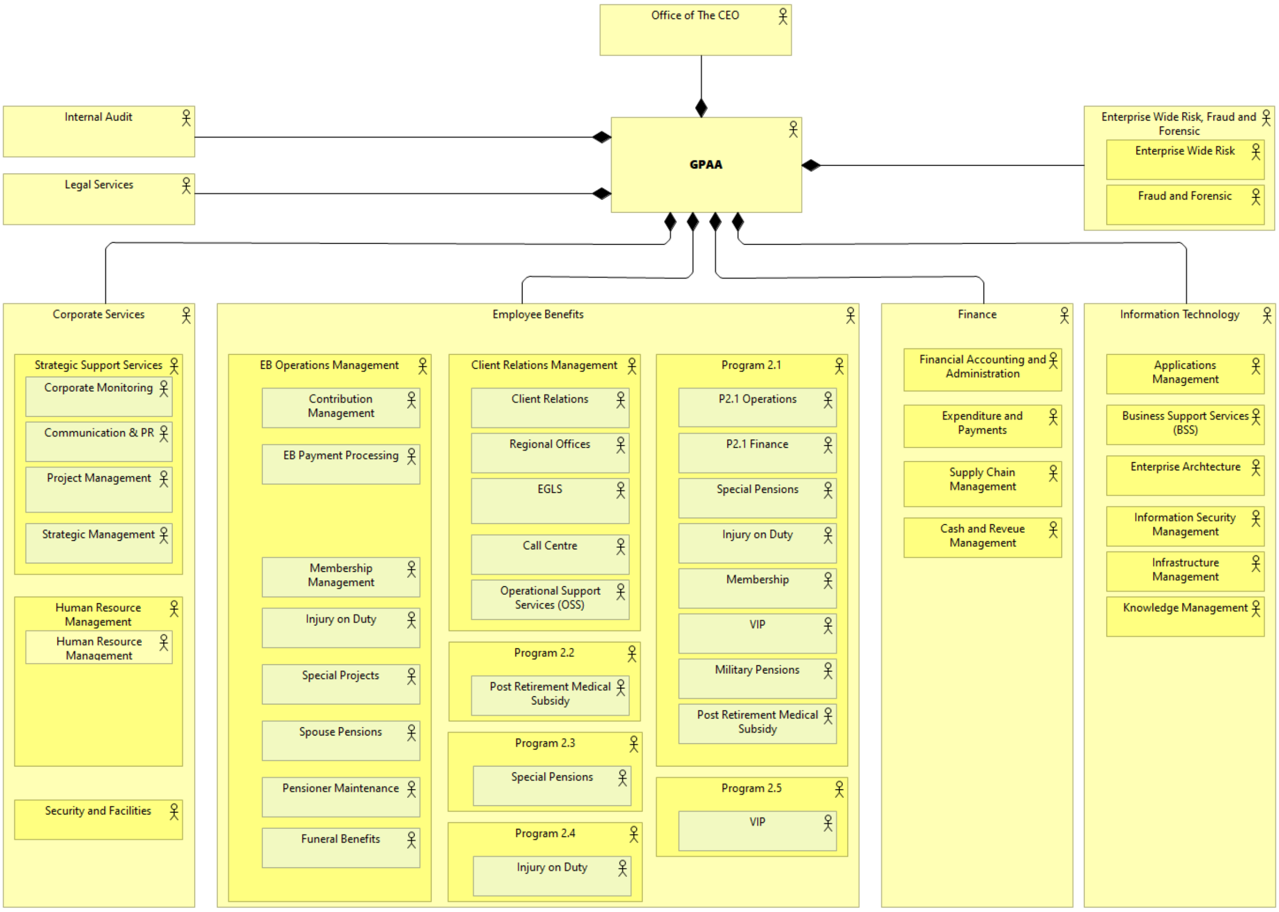


Figure 6 GPAA Current Organizational Functions View

Future Interim Structure: The is the proposed organizational view and structure is shown below.

This structure aligns to the organisational strategy.

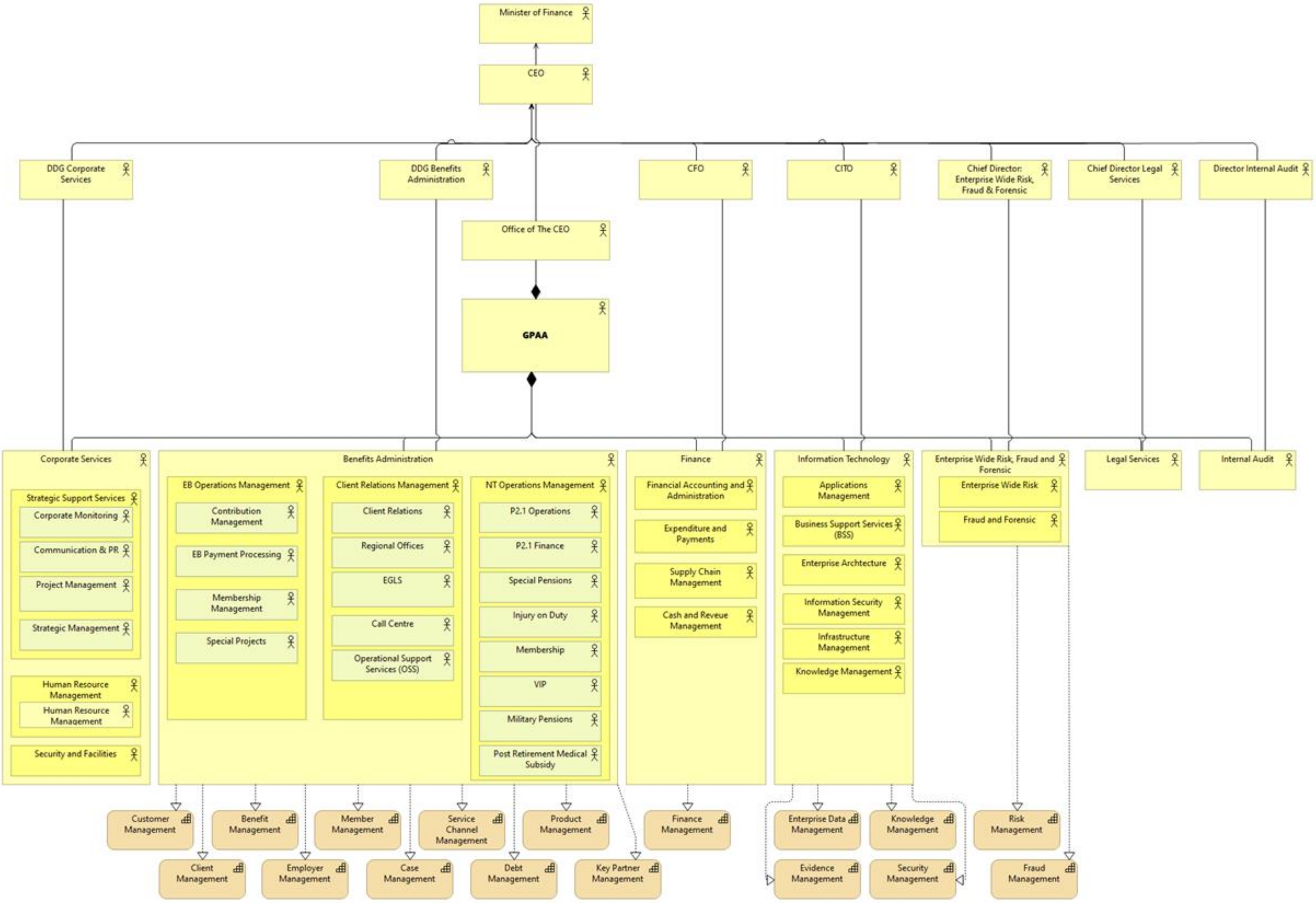


Figure 7 GPAA Proposed Organizational View

Understanding the GPAA Business Units and Departments

The Core Business Units

The GPAA core business is divided into several key units and functions, mostly within Benefits Administration business unit, each catering to specific capabilities within the overall capability model. These units are designed to function cohesively and support the overarching goals of the organization.

The Supporting Departments

In addition to the core business units, various supporting departments are aligned to enhance the efficiency and functionality of the GPAA. This hierarchical structure should create a seamless flow of operations, thereby enhancing performance. These include and Corporate Services, Finance, IT, Risk, egal and Internal Audit.

The Modernisation Programme: A Multi-Stage Approach

Stages and Impact

The Modernisation Programme shall influence multiple areas of the organization through different stages of its roadmap. This approach ensures that the transition is gradual, planned, managed and in alignment with the evolving needs of the business.

Objectives and Compatibility

Most of the current functions within the organization are deemed sufficient to support the primary objectives of the Modernisation Programme. However, this is not a static assessment but one that will evolve as per the strategies and requirements laid down by the GPAA.

Adapting to Change: Flexibility in Structure

Subject to Alteration

The depicted GPAA structure is not set in stone. It is formulated with the understanding that change is inevitable and is influenced by various factors. The alignment and collaboration of business units should continually be reviewed and adjusted through ongoing and future initiatives.

It is important to note that the current structure is subject to public service regulation and cannot be changed without proper consultation and approval. This is a serious constraint that must always be considered.

Reviewing Business and Operating Models

The GPAA is engaging in ongoing of the review of its Business and Operating Models. This not only ensures that the structure remains relevant but also anticipates shifts in the industry landscape, thereby preparing the organization for future challenges.

Exceptions and Responsibilities in the Capability Model

The Unmapped Capabilities

Certain capabilities within the GPAA, such as Enterprise Data Management, are yet to be assigned a responsible functional team. These exceptions should be acknowledged and incorporated into a proactive approach to continually refine the structure.

Future Mapping and Strategy Alignment

The defined business units mapped to support the proposed capability model are well-structured. However, this alignment shall continue to be informed and guided by evolving strategies within the GPAA. The focus is not merely on present functionality but also on future adaptability.

The GPAA Organizational Structure is a thoughtful blueprint that balances the need for stability with the demands of modernization. With a clear understanding of its business units, a phased approach to modernization, and a keen eye on future needs and challenges, the GPAA is strategically poised to not only meet its current objectives but also to adapt and thrive in an ever-changing business environment.

3.1.7 **Capabilities**

Enterprise capabilities refer to the abilities, skills, technologies, processes, and tools that an organization possesses to achieve its business goals, particularly in the context of complex and large-scale operations. These capabilities enable an organization to provide value to its customers, compete effectively in the market, and achieve long-term success.

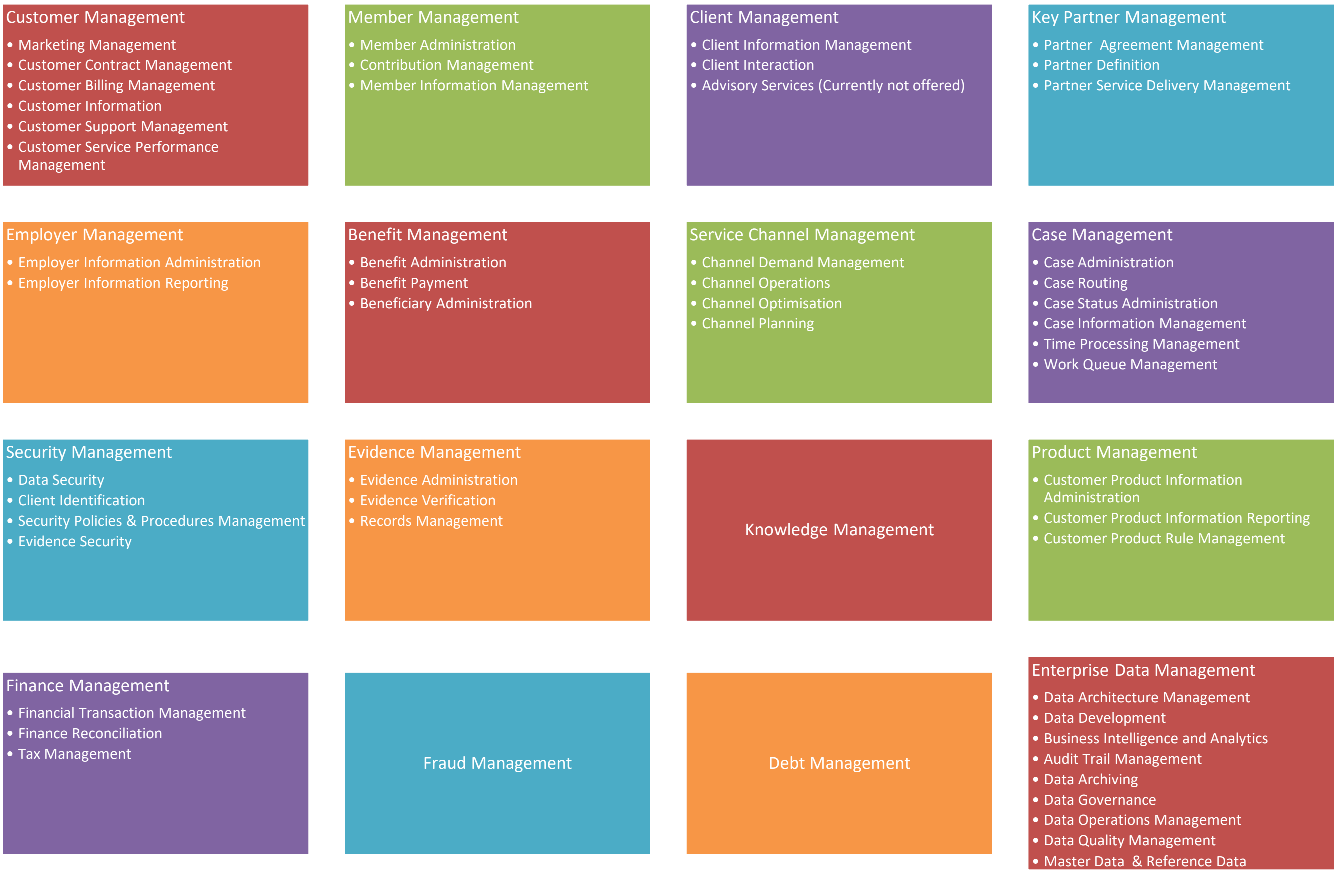
GPAA has defined Business Capabilities at three levels – L1, L2 and L3.

A high-level view of the capability model of the GPAA is presented in the diagram below. capabilities are provided showing the L1 and L2 Capabilities.

The L1, L2 and L3 Capabilities have been defined in separate artefacts and in the EA Model and Repository.

These Capabilities support the Value Streams that the GPAA embraces.

These are also mapped to the Business Organizational Units and to the Value Streams.



Customer Management
- Marketing Management
- Customer Contract Management
- Customer Billing Management
- Customer Information
- Customer Support Management
- Customer Service Performance Management

Member Management
- Member Administration
- Contribution Management
- Member Information Management

Client Management
- Client Information Management
- Client Interaction
- Advisory Services (Currently not offered)

Key Partner Management
- Partner Agreement Management
- Partner Definition
- Partner Service Delivery Management

Employer Management
- Employer Information Administration
- Employer Information Reporting

Benefit Management
- Benefit Administration
- Benefit Payment
- Beneficiary Administration

Service Channel Management
- Channel Demand Management
- Channel Operations
- Channel Optimisation
- Channel Planning

Case Management
- Case Administration
- Case Routing
- Case Status Administration
- Case Information Management
- Time Processing Management
- Work Queue Management

Security Management
- Data Security
- Client Identification
- Security Policies & Procedures Management
- Evidence Security

Evidence Management
- Evidence Administration
- Evidence Verification
- Records Management

Knowledge Management

Product Management
- Customer Product Information Administration
- Customer Product Information Reporting
- Customer Product Rule Management

Finance Management
- Financial Transaction Management
- Finance Reconciliation
- Tax Management

Fraud Management

Debt Management

Enterprise Data Management
- Data Architecture Management
- Data Development
- Business Intelligence and Analytics
- Audit Trail Management
- Data Archiving
- Data Governance
- Data Operations Management
- Data Quality Management
- Master Data & Reference Data

Figure 8 GPAA L1 & L2 Capabilities

3.1.8 **Operating Model Considerations**

A target operating model (TOM) is a blueprint or a framework that describes how an organization plans to operate in the future to achieve its strategic objectives. It is a high-level representation of the desired state of an organization's structure, processes, capabilities, and technology.

The TOM shall need to be defined and it should cover areas below.

- Organizational Structure
- Processes
- Roles and Responsibilities
- People & Culture
- Governance and Decision-Making
- Capabilities and Skills
- Technology and Infrastructure
- Performance Management

It has been agreed that the design of a Target Operating Model is out of scope for this work package as it is an exercise that require a lot more stakeholders, effort, and time. This work package does not have sufficient time to cover the revision of the Business Operating Model in detail. The work package will however deliver on some aspects of the TOM.

Target Operating Model Factors for consideration and an Operating Model Canvas and have however been incorporated in the document.

3.1.9 Legislative Mandates

The various benefits administered by GPAA are governed by a variety of acts, each of which has an impact on how these benefits are handled and the corresponding services supplied. The GPAA currently administers the following funds and schemes, as well as the applicable legislation that governs these programmes:

Funds and Schemes:	Applicable legislation:	Administered on behalf of:
Government Employees Pension Fund (GEPF)	Government Employees Pension Law of 1996	GEPF's Board of Trustees
Temporary Employees Pension Fund (TEPF)	Temporary Employees Pension Fund Act 75 of 1979	National Treasury's Programme 7
Associated Institutions Pension Fund (AIPF)	Associated Institutions Pension Fund Act 41 of 1963	National Treasury's Programme 7
Military Pensions	Military Pensions Act 84 of 1976	National Treasury's Programme 7
Injury on Duty payments	Compensation for Occupational Injuries and Diseases Act 130 of 1993	National Treasury's Programme 7
Special Pensions	Special Pensions Act 69 of 1996	National Treasury's Programme 7
Post-Retirement Medical Subsidies	Public Service Co-Ordinating Bargaining Council (PSCBC) resolutions; as provided for and regulated	National Treasury's Programme 7

Table: Legislation that governs schemes and funds administered by the GPAA.

The GPAA's financial affairs are governed by the Public Finance Management Act (PFMA), while its human resources fall under the ambit of the Public Service Act (PSA).

The COFI Bill

The Conduct of Financial Institutions (COFI) Bill. The COFI Bill aims to significantly streamline the legal landscape for conduct regulation in the financial sector, and to give legislative effect to the market conduct policy approach.

The bill requires financial institutions to provide consumers with clear information about their services, their fees, and the risks associated with their products.

For the GPAA and its customers and partners, this means adapting to enhanced regulatory requirements. The associated Funds will now have to be licensed under the Pension Funds Act and under COFI and the same principles and requirements will apply.

The GPAA may be influenced in various ways including those below, some of which can be implemented through the Modernisation Programme:

- **Transparency & Communication**: The GPAA will need to ensure clear communication about services, fees, and risks to its members, enhancing trust and stakeholder relations. Communications, awareness and education may need to be conducted for clients.

- **Compliance & Reporting**: Adherence to the new regulatory landscape will necessitate updates to compliance protocols and reporting mechanisms.
- **Operational Adjustments**: The introduction of the new regulations may lead to operational changes aimed at aligning with the bill’s requirements.
  The Target Operating Model and Governance processes shall need to be defined and modelled to clearly to always show compliance with the requirements of the bill.
- **Risk Management**: Clear articulation of risks associated with pension products will be crucial, necessitating adjustments in risk management strategies.
- **Data & Information Management**: To support compliance with the Bill, the data and information management capabilities shall need to be enhanced and be able to provide accurate relevant information for stakeholders as and when required. Changes to terminology or naming conventions for products and schemes may need to be applied onto existing and incoming data.

  Prioritization of the data capabilities is necessary.
- **Information Channels**: Relevant information shall need to be made available through various digital and physical channels that are accessible to clients. The updating of relevant information may also need to be catered for seamlessly.

The Two-Pot Retirement Saving System

The government is planning a two-pot retirement system which is meant to assist people to help cope with challenging financial situations. This will allow for limited withdrawals of up to a third of one's retirement funds.

The impact of the change shall need to be assessed further and the necessary adjustments made. This may include the following.

Impact on GPAA Operations: The GPAA (Government Pensions Administration Agency) will likely see an **increase in administrative tasks**, given that individuals can access one-third of their retirement savings throughout their career. This might necessitate more personnel or **streamlined processes** to handle withdrawal requests and ensure compliance with the new rules.

Technological Support: Technology can play a crucial role in automating and streamlining the additional processes resulting from the two-pot system. Implementation of digital platforms for **request processing**, **real-time tracking of fund values**, and **automated compliance checks** can help in managing the increased workload efficiently.

3.1.10 GPAA Operating Model Canvas

The operating model canvas is a visual tool that is used to translate a strategy into operational choices. It gives a high-level overview of the current operations and helps in designing the detailed work processes. The Operating Model can be depicted using various tools and visual representations.

The GPAA operating model depicted below takes the value chains for core business operations as per the GPAA Strategy and shows the various enabling components and collaborators that enable realization of the organization’s operational mandates. It essentially expands upon the Value Chain, Key Resources, and Key Partners of the Business Model.

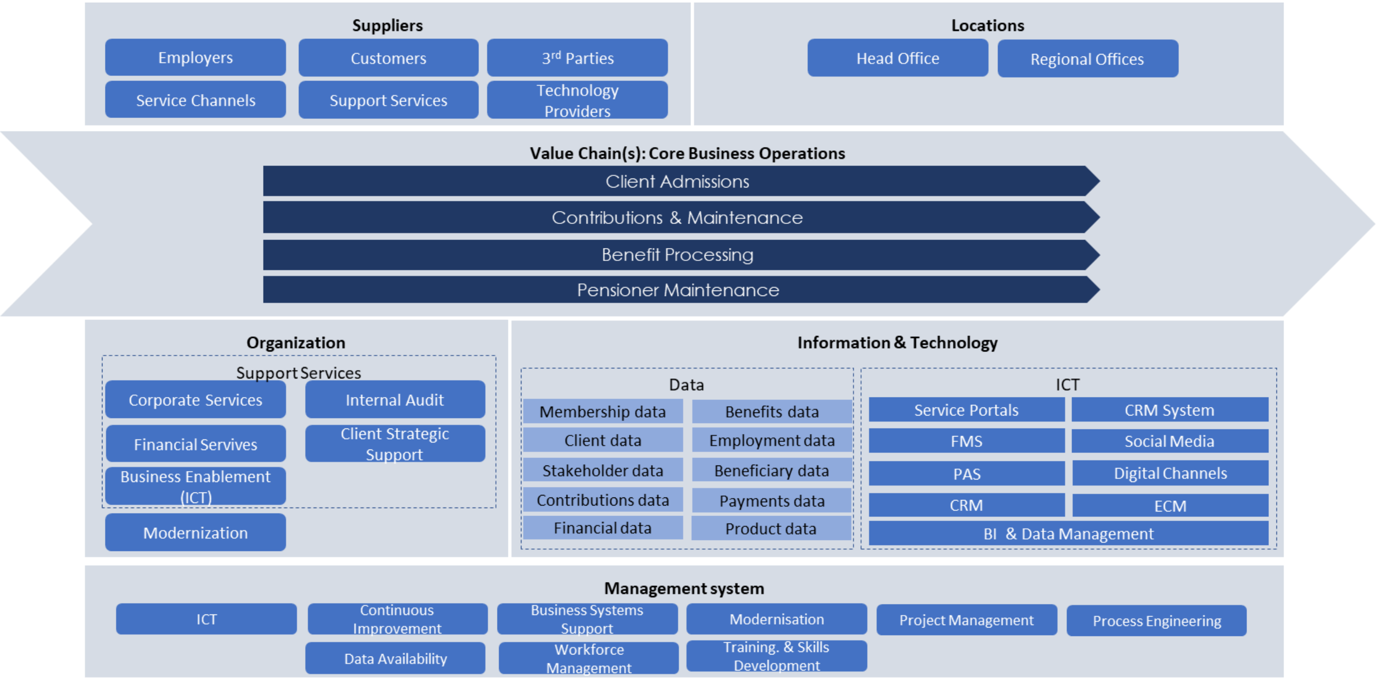


Figure 9 GPAA Operating Model Canvas

Organizational Engagement & Collaboration

The Government Pensions Administration Agency has a complex network of interactions with various governmental bodies, financial institutions, service providers, and individuals to effectively manage and administer pension benefits for government employees in South Africa. These interactions are crucial for the smooth operation of the pension system and ensuring that pensioners receive their benefits in a timely and accurate manner.

The diagram below depicts some of the entities that engage with the GPAA within it’s value network as stated in the Business Model.

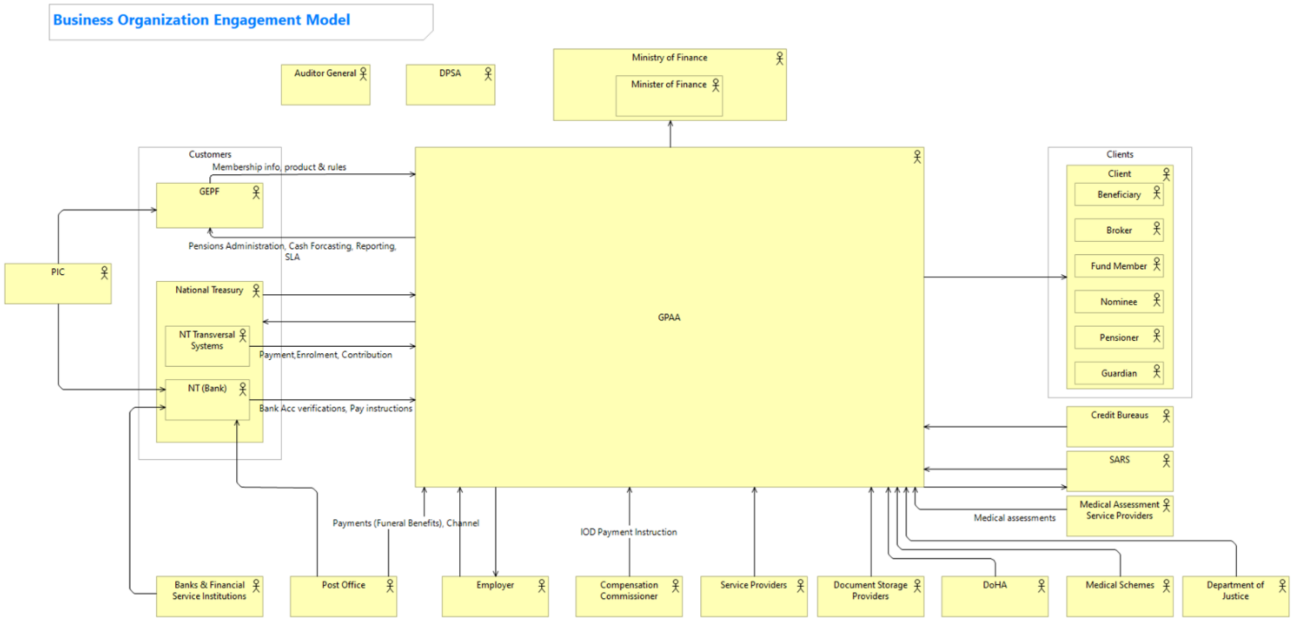

Business Organization Engagement Model
Auditor General
DPSA
Ministry of Finance
Minister of Finance
Customers
Membership info, product & rules
GEPF
Pensions Administration, Cash Forcasting, Reporting, SLA
PIC
National Treasury
NT Transversal Systems
Payment,Enrolment, Contribution
NT (Bank)
Bank Acc verifications, Pay instructions
GPAA
Clients
Client
Beneficiary
Broker
Fund Member
Nominee
Pensioner
Guardian
Credit Bureaus
SARS
Medical Assessment Service Providers
Medical assessments
Payments (Funeral Benefits), Channel
IOD Payment Instruction
Banks & Financial Service Institutions
Post Office
Employer
Compensation Commissioner
Service Providers
Document Storage Providers
DoHA
Medical Schemes
Department of Justice

Figure 10 GPAA Organizational Engagement & Collaboration

GPAA's Customers are the GEPF and National Treasury, for whom the organisation provides administration services.

It is acknowledged that although GPAA serves the depicted Clients, these are clients of the associated Pension Funds and that is where the relationship is held.

The following provides context on the engagement between GPAA and the entities that the organisation engages and collaborates with.

Entity	Relationship	Considerations
Ministry of Finance	GPAA operates under the authority and guidance of the Ministry of Finance, which sets the overall policies and budget for government pensions. GPAA provides regular reports and financial data to the Ministry of Finance for budgetary planning and oversight.	
GEPF	GPAA administers pension benefits on behalf of GEPF. GPAA interacts closely with GEPF to ensure accurate record-keeping and timely disbursement of pension benefits to government employees.	
National Treasury	GPAA collaborates with the National Treasury to align its financial operations with government fiscal policies. GPAA may require approvals and financial allocations from the National Treasury for its operations.	

Banks & Financial Service Institutions	GPAA partners with banks and financial institutions to facilitate the distribution of pension payments to beneficiaries. These institutions often provide the necessary financial infrastructure for electronic fund transfers.	
Post Office	GPAA may use the postal services, including registered mail, to communicate with pensioners and beneficiaries. The Post Office may also be involved benefit payments.	
Employers	GPAA may use the postal services, including registered mail, to communicate with pensioners and beneficiaries. The Post Office may also be involved in the distribution of physical pension checks.	
Compensation Commissioner	GPAA may coordinate with the Compensation Commissioner when handling pension matters related to workplace injuries and compensation claims.	
Service Providers	GPAA engages various service providers, such as IT companies and consulting firms, to maintain and improve its pension administration systems.	
Document Storage Providers	GPAA relies on document storage providers for the secure storage and retrieval of pension-related documents and records.	
Department of Home Affairs (DHA)	GPAA may require information from the Department of Home Affairs for identity verification and beneficiary data.	
Medical Schemes	GPAA may interact with medical schemes when processing healthcare-related claims for pensioners and beneficiaries.	
Department of Justice	GPAA may engage with the Department of Justice in cases involving legal matters related to pension benefits or disputes.	
Medical Assessment Service Providers	GPAA may collaborate with medical assessment service providers to assess and verify medical claims for disability benefits.	
South African Revenue Service (SARS)	GPAA interacts with SARS to ensure tax compliance and accurate withholding tax on pension benefits.	
Credit Bureaus	GPAA may report pension-related information to credit bureaus if pensioners have outstanding loans or credit obligations.	
Clients	GPAA communicates regularly with members, beneficiaries, and pensioners to provide information, updates, and resolve inquiries related to their pensions.	

Department of Public Service and Administration (DPSA)	GPAA may coordinate with the DPSA regarding policy changes, updates, and the implementation of pension-related regulations for public servants.	
Auditor General	The Auditor General conducts audits of GPAA's financial and operational processes to ensure transparency and compliance with government regulations.	

Stakeholder Engagement

The GPAA reports to the Minister of Finance and its mandate is to administer pensions on behalf of GEPF and National Treasury. The GPAA fulfils an administrative role for the two customers.

The establishment of the GPAA is an alignment of pension's administration in government to an industry practice where pension funds are administered by agencies outside of the funds.

The organisation's stakeholders, its core services and the interactions associated with each person / group, are as indicated on table below.

Stakeholder	Core services provided / interaction points
Internal Stakeholders	
Audit and Risk Management Committees	Provide internal audit reports and assurance on the risk management controls and governance process of the GPAA
EXCO	Conducts regular meetings to discuss work flow, dashboard matters, and risk and fraud management
MANCO	Proposes operational changes and improvements to EXCO
GPAA middle management and officials	Conduct planning, policy development and performance reporting; and Provide comprehensive human resources services
External Stakeholders	
Auditor-General	Provides performance information. Respond to audit findings
Cabinet	Addresses cabinet memoranda and legislation
Government departments and Parliament	Provide administrative support for the department in terms of responding to Parliamentary questions, Cabinet memoranda and requests from government departments

National Treasury and GEPF	Facilitate the process for the approval of the Annual Performance Plans, the Strategic Plan; Provides assistance on PFMA compliance issues; Engages on budget options, funding of policy priorities and quarterly meetings of chief audit executives
Offices of the Minister and Deputy Minister of Finance and Director-General of National Treasury	Provide information (in the form of briefing notes, submissions or presentations) and support in relation to the governance and finance. Holds regular meetings to discuss work flow, dashboard matters, and risk and fraud management.
Parliamentary Engagement	PEOW should be notified well in advance prior to engagement
Portfolio Committees	Brief on the Corporate Strategy, Annual Report and policy priorities

Table 2: Stakeholder analysis

3.1.11 **Value Streams**

Value streams refer to the series of steps that an organization uses to create and deliver a product or service to a customer.

The purpose of defining value streams is to understand and visualize the entire process of delivering a product or service to the customer.

This involves identifying and mapping out the series of processes and activities required to deliver pension services to government employees and beneficiaries.

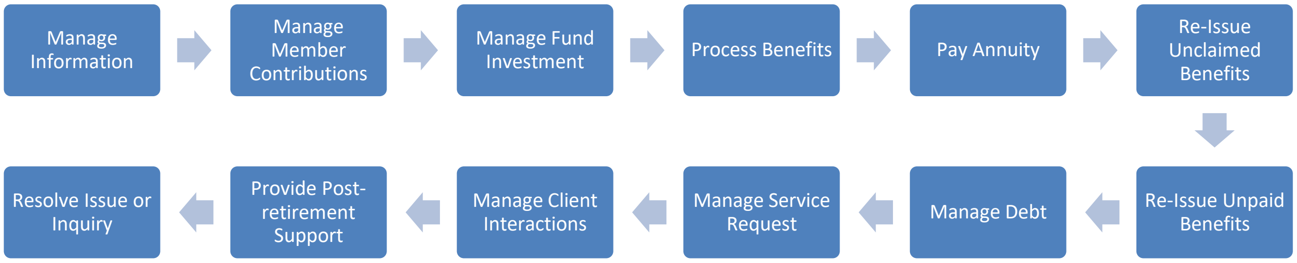
Defining value streams for the GPAA helps in improving efficiency, compliance, transparency, alignment with strategic goals, beneficiary satisfaction, and overall risk management, leading to more effective and accountable pension administration.

They provide a high-level description of the value stages making up the value streams that enable the GPAA to carry out its mandate.

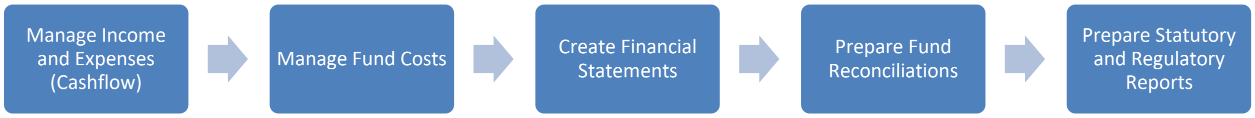
The core Value Streams have been defined and revised to support the core business functions of the organisation.

The diagrams that follow below provide a view of GPAA’s value streams.

Core Value Stream:



Administrative Value Stream


Manage Income and Expenses (Cashflow)
Manage Fund Costs
Create Financial Statements
Prepare Fund Reconciliations
Prepare Statutory and Regulatory Reports

Below is further decomposition of the Core Value Streams.

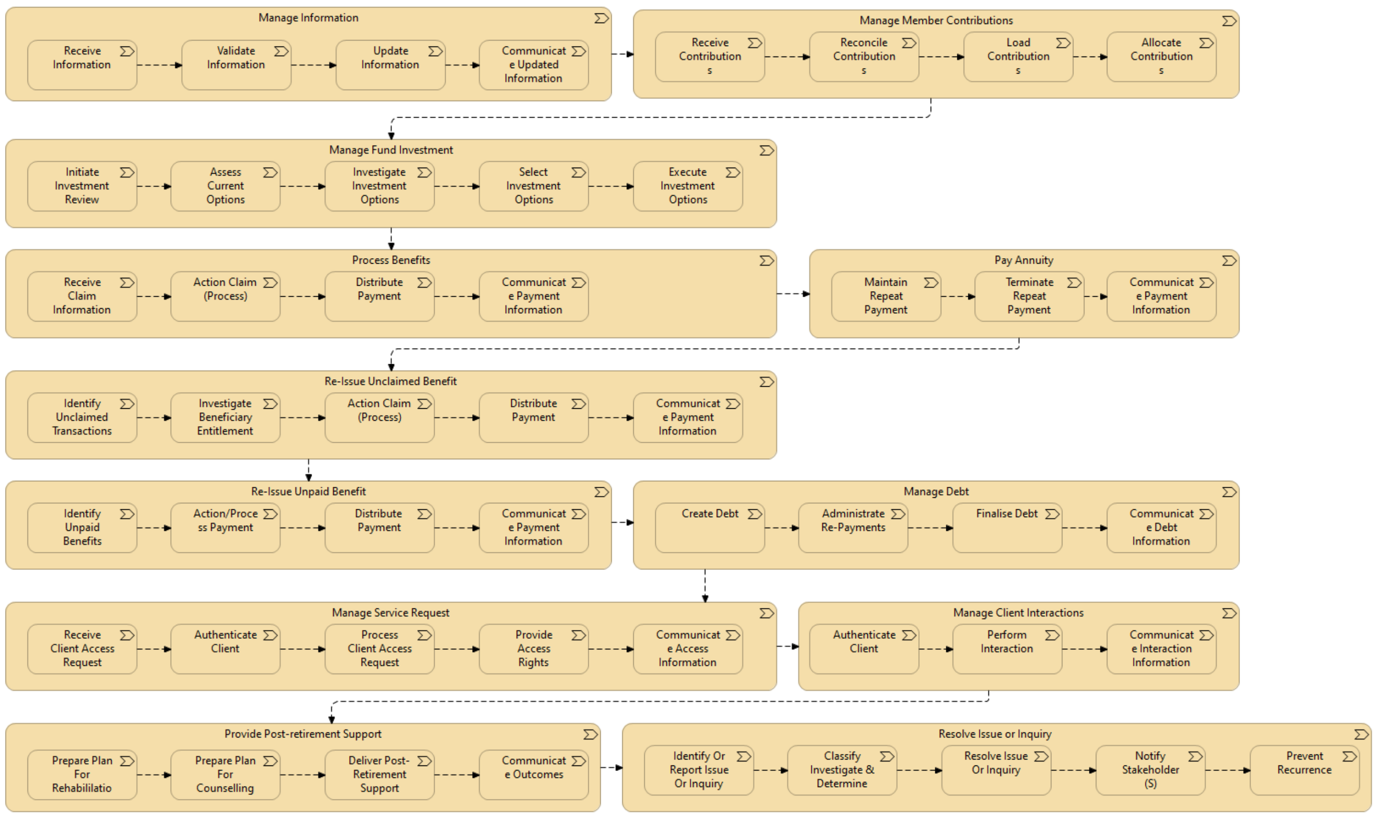

Manage Information
Receive Information
Validate Information
Update Information
Communicate Updated Information
Manage Member Contributions
Receive Contributions
Reconcile Contributions
Load Contributions
Allocate Contributions
Manage Fund Investment
Initiate Investment Review
Assess Current Options
Investigate Investment Options
Select Investment Options
Execute Investment Options
Process Benefits
Receive Claim Information
Action Claim (Process)
Distribute Payment
Communicate Payment Information
Pay Annuity
Maintain Repeat Payment
Terminate Repeat Payment
Communicate Payment Information
Re-Issue Unclaimed Benefit
Identify Unclaimed Transactions
Investigate Beneficiary Entitlement
Action Claim (Process)
Distribute Payment
Communicate Payment Information
Re-Issue Unpaid Benefit
Identify Unpaid Benefits
Action/Process Payment
Distribute Payment
Communicate Payment Information
Manage Debt
Create Debt
Administrate Re-Payments
Finalise Debt
Communicate Debt Information
Manage Service Request
Receive Client Access Request
Authenticate Client
Process Client Access Request
Provide Access Rights
Communicate Access Information
Manage Client Interactions
Authenticate Client
Perform Interaction
Communicate Interaction Information
Provide Post-retirement Support
Prepare Plan For Rehabililatio
Prepare Plan For Counselling
Deliver Post-Retirement Support
Communicate Outcomes
Resolve Issue or Inquiry
Identify Or Report Issue Or Inquiry
Classify Investigate & Determine
Resolve Issue Or Inquiry
Notify Stakeholder (S)
Prevent Recurrence

Figure 11: GPAA's Core Value Streams

Below is a decomposition of the Administrative Value Streams, showing the value stages.

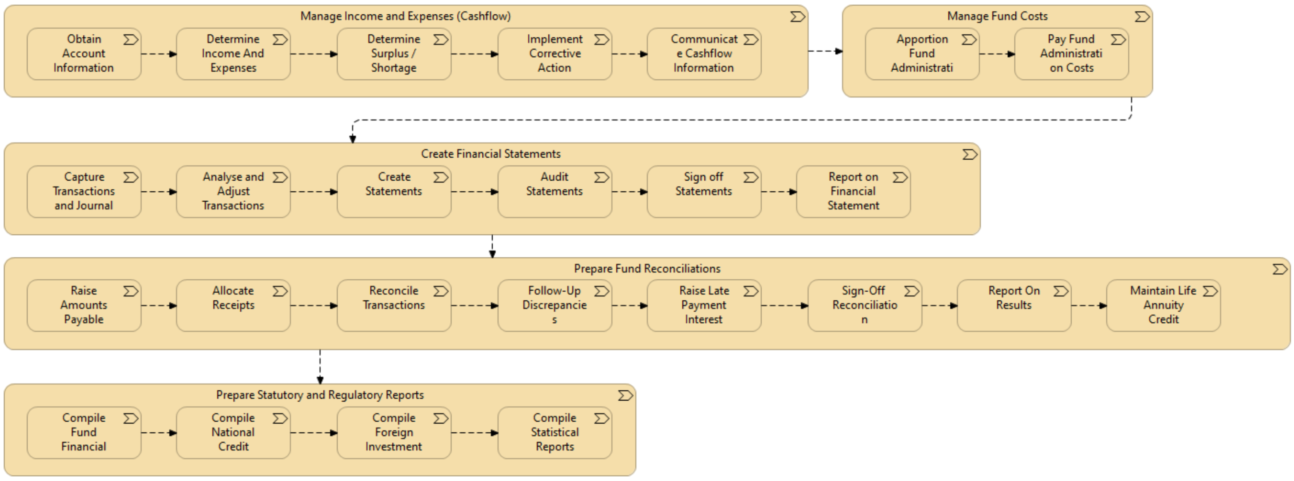

Manage Income and Expenses (Cashflow)
Obtain Account Information
Determine Income And Expenses
Determine Surplus / Shortage
Implement Corrective Action
Communicate Cashflow Information
Manage Fund Costs
Apportion Fund Administration Costs
Pay Fund Administration Costs
Create Financial Statements
Capture Transactions and Journal
Analyse and Adjust Transactions
Create Statements
Audit Statements
Sign off Statements
Report on Financial Statement
Prepare Fund Reconciliations
Raise Amounts Payable
Allocate Receipts
Reconcile Transactions
Follow-Up Discrepancies
Raise Late Payment Interest
Sign-Off Reconciliation
Report On Results
Maintain Life Annuity Credit
Prepare Statutory and Regulatory Reports
Compile Fund Financial
Compile National Credit
Compile Foreign Investment
Compile Statistical Reports

Figure 12 GPAA's Administrative Value Streams

The value streams are further detailed by business processes that are tangible processes enabling the GPAA to fulfil its mission. To-be processes are currently being defined and these shall be mapped to the value streams.

3.1.12 Business Processes

A business process at its core is a sequence of steps or activities to achieve a specific outcome that delivers or contributes to value.

Each step in a business process usually represents an assigned task, implementing business capabilities.

The GPAA Business Processes have been mapped to the business functions and to the value streams.

The GPAA To-Be Business Processes are still to be defined and shall be modelled accordingly in the repository once defined.

Business Process Value Stream Mapping

The following table maps the Core Business processes to the Value streams and business function.

Value Stream	Process	Business Section / Component
Manage Claim	Claim Resignation Benefit - GEPF	EB Withdrawals
	Claim Retirement Benefit - GEPF	EB Withdrawals
	Claim Discharge Benefit - GEPF	EB Withdrawals
	Claim Death Benefit - GEPF	EB Withdrawals
	Claim Resignation Benefit - NSF	Special Projects
	Claim Retirement Benefit - NSF	Special Projects
	Claim Discharge Benefit - NSF	Special Projects
	Claim Death Benefit - NSF	Special Projects
	Claim Funeral Benefit - GEPF	Pensioner Maintenance
	Claim Funeral Benefit - GEPF	Funeral Benefits
	Claim Funeral Benefit - NT	Special Pensions
	Claim Funeral Benefit - NT	Military Pensions
	Claim Funeral Benefit - NT	VIP
	Claim 5 year balance - Death - GEPF	Special Projects
	Claim Clean Break Settlement (Divorce Benefit) - GEPF	Special Projects
	Claim Injury on Duty (Member) - NT	IOD
	Claim VIP & PSOP - NT	VIP
	Claim VIP (Spouse) - NT	VIP
	Claim VIP (Child) - NT	VIP
	Claim Military Medical (MM) Pension - NT	Military Pensions
	Claim Military Pension (Member) - NT	Military Pensions
	Claim Military Pension (Spouse) - NT	Military Pensions
	Claim Medical Expense - NT	Medical Account
	Claim Medical Subsidy (Monthly) - NT	Post Medical Benefits
	Claim Medical Subsidy (Once-off) - NT	Post Medical Benefits

	Claim spouse pensions - GEPF	EB Withdrawals
	Claim spouse pensions - NT	Special Pensions
	Claim spouse pensions - NT	IOD
	Claim child pensions - NT	IOD
	Claim Special pensions (Member) - NT	Special Pensions
	Claim Special pensions (Spouse) - NT	Special Pensions
	Claim Special pensions (Child) - NT	Special Pensions
	Claim PDP - GEPF	Special Projects
	Claim NSF - GEPF	Special Projects
	Claim divorce (retirements/death/resignation) - GEPF	Special Projects
	Claim General Assistance cases - GEPF	Special Projects
	Claim Ex Cape teachers - GEPF	Special Projects
	Claim Supported Employment Enterprises cases - GEPF	Special Projects
	Claim discharge - GEPF	EB Withdrawals
	Claim Special Benefits (HODs) - GEPF	EB Withdrawals
	Claim Special Benefits (> 7yr)- GEPF	EB Withdrawals
	Claim Special Benefits (Old fund)- GEPF	EB Withdrawals
	Claim Special Benefits (>2000K) - GEPF	EB Withdrawals
	Claim child pensions - GEPF	EB Withdrawals
	Claim TEPF resignation - GEPF	TEPF
	Claim TEPF Misconduct - GEPF	TEPF
	Claim TEPF ill-health - GEPF	TEPF
	Claim TEPF retirement more than 10 years - GEPF	TEPF
	Claim TEPF retirement less than 10 years - GEPF	TEPF
	Claim AIPF resignation - GEPF	AIPF
	Claim AIPF misconduct - GEPF	AIPF
	Claim AIPF ill-health - GEPF	AIPF
	Claim AIPF retirement more than 10 years - GEPF	AIPF
	Claim AIPF retirement less than 10 years - GEPF	AIPF
	Claim Graduity - GEPF	EB Withdrawals
	Claim 3rd pensions - GEPF	Pensioner Maintenance
	Claim Orphan and Child Pensions - GEPF	Pensioner Maintenance
	Claim re-calculated benefits - GEPF	Pensioner Maintenance
	Claim re-distributed benefits - GEPF	Pensioner Maintenance
	Claim Demilitarized cases - GEPF	Special Projects
	Claim unclaimed benefits - GEPF	Unclaimed Benefits and Re-issue
	Interface (transversal)	
	Interface with SARS - GEPF	GEPF Funds
	Interface with SARS (VIP, PDP, NSF and Special Pensions) - NT	NT funds
	Interface with Home Affairs - GEPF	GEPF Funds
	Interface with Home Affairs (VIP, PDP, NSF and Special Pensions) - NT	NT funds
	Interface with SafetyWeb- GEPF	GEPF Funds

	Interface with SafetyWeb (VIP, PDP, NSF and Special Pensions) - NT	NT funds
	Interface with Bank Validation- GEPF	GEPF Funds
	Interface with Bank Validatio(VIP, PDP, NSF and Special Pensions) - NT	NT funds
Manage Payment	Manage Bank Payments - GEPF benefits	GEPF Funds
	Manage Bank Payments - NT benefits	NT Funds
	Manage Post Office payments - GEPF	GEPF Funds
	Manage Post Office payments - NT	NT Funds
	Manage Post Office payment cancellations - GEPF	GEPF Funds
	Manage Post Office payment cancellations - NT	NT Funds
	Manage Tax payments - GEPF	GEPF Funds
	Manage Tax payments - NT	NT Funds
	Manage telegraphic Transfer payments - GEPF	GEPF Funds
	Manage telegraphic Transfer payments - NT	NT Funds
	Prepare and review general ledger reconciliations for TEPF, AIPF and GEPF	EB Accounts
	Prepare and review general ledger reconciliations for IOD,Special pensions, Post medical benefits, Military Pensions, Medical Accounts, VIP	NT Funds
	Calculate and authorise interest payments not calculated by the system	GEPF Funds
	Calculate and authorise interest payments not calculated by the system	NT Funds
	Create and confirm DIRCO payments	EB Accounts
	Prepare cash flow for payments of benefits - GEPF	GEPF Funds
	Prepare cash flow for payments of benefits - NT	NT Funds
	Pay IOD Benefits between 1-30% of PD (lump sum) - NT	IOD
	Pay once(off) payment to member not qualify for subsidy - NT	Post Medical Benefits
	Pay military medical account - NT	Military Medical Account
	Pay 5yr balances	Pensioner Maintenance
	Pay 3rd pensions - GEPF	Pensioner Maintenance
	Pay re-calculated benefits - GEPF	Pensioner Maintenance
	Pay re-distributed benefits - GEPF	Pensioner Maintenance
	Pay PDP cases - GEPF	Special Projects
	Pay clean break cases - GEPF	Special Projects
	Pay divorce (retirements/death/resignation) - GEPF	Special Projects
	Pay Supported Employment Enterprises cases - GEPF	Special Projects
	Pay Demilitarized cases -GEPF	Special Projects
	Pay discharge	EB Withdrawals
	Pay transfer (owner or FSB recognized entity) - GEPF	Pensioner Maintenance
	Pay funeral benefits - GEPF	Funeral Benefits
	Pay funeral benefits (subjected to approval of the Chief Medical Officer) - NT	Military Pensions
	Pay VIP funeral benefit - NT	VIP
	Pay Special Pension funeral benefits -NT	Special Pensions

	Pay Retirement - GEPF	Pensioner Maintenance /EB Withdrawals
	Pay IOD Benefits between 31-100% of PD(monthly till death)- NT	IOD
	Pay death on duty benefits to spouse and/or child (monthly till death) - NT	IOD
	Pay Post Medical Benefits Monthly - NT	Post Medical Benefits
	Pay military pension benefits - NT	Military Pension
	Pay spouse benefits - NT	Military Pension
	Pay VIP benefits (Member) - NT	VIP
	Pay VIP benefits (Spouse) - NT	VIP
	Pay VIP benefits (Child) - NT	VIP
	Pay special pension benefits - NT	Special Pensions
	Pay special pension benefits (beneficiary) - NT	Special Pensions
	Pay Orphan and Child Pensions - GEPF	Pensioner Maintance
	Pay NSF cases - GEPF	Special Projects
	Pay Ciskei strike cases - GEPF	Special Projects
	Pay General Assistance cases - GEPF	Special Projects
	Pay Ex Cape teachers - GEPF	Special Projects
	Pay Supported Employment Enterprises cases - GEPF	Special Projects
	Pay Demilitarized cases - GEPF	Special Projects
	Pay discharge - GEPF	EB Withdrawals
	Pay Special Benefits (HODs) - GEPF	EB Withdrawals
	Pay Special Benefits (> 7yr)- GEPF	EB Withdrawals
	Pay Special Benefits (Old fund)- GEPF	EB Withdrawals
	Pay Special Benefits (>2000K) - GEPF	EB Withdrawals
	Pay TEPF retirement more than 10 years - GEPF	TEPF
	Pay TEPF retirement more than 10 years - GEPF	TEPF
	Pay TEPF retirement less than 10 years - GEPF	TEPF
	Pay AIPF ill-health - GEPF	AIPF
	Pay AIPF retirement more than 10 years - GEPF	AIPF
	Pay AIPF retirement less than 10 years - GEPF	AIPF
	Create and confirm DIRCO payments	EB Finance
	Create and confirm requested tax payments	EB Finance
Manage Annuity Increase	implement medical tariffs increase and subsidy increases - NT	Post Medical Benefits
	Implement VIP pensions annual increase - NT	VIP
	Implement Special pensions annual increase - NT	Special Pensions
	Implement GEPF pensions annual increase - GEPF	GEPF funds
	Implement TEPF pensions annual increase - GEPF	TEPF fund
	Implement AIPF pensions annual increase - GEPF	AIPF fund
Manage Member contribution	facilitate collection and reconciliation of contribution	Contributions
	Develop contribution reports	Contributions
	Processing FinRecon (Electronic Contributors)	Contributions
	Processing manual Contribution billing	Contributions

	Processing purchase of Service Run (POS) Run reconciliation	Contributions
	Processing additional Liabilities;	Contributions
	Handle pensionable Salary confirmations, Contribution Queue.	Contributions
	Develop contribution management reports	Contributions
Manage Re-Issue and Unclaimed Benefit	Trace beneficiaries - GEPF	Finance
	Re-issue benefits - GEPF	Finance
	Identify Unclaimed Benefits	Finance
	Investigate Beneficiary Entitled	Finance
	Action/Process Payment	Finance
	Distribute Payment	Finance
	Communicate Payment Information	Finance
Manage debt (Benefit)	Manage employer debt outstanding contribution - GEPF	Contributions
	Manage departmental debt (claim from employer department against a member (e.g busary or loan)) - GEPF	Contributions
	Manage member debt (member outstanding contribution)- GEPF	Membership
	Manage Overpayment (GEPF funds)- GEPF	Pensioner Maintance/Disallowances
	Manage Overpayment (NT funds)- NT	NT Finance/Disallowances
	Manage Underpayments (GEPF Funds) - GEPF	Pensioner Maintance/Disallowances
	Manage Underpayments (NT Funds) - NT	NT Finance/Disallowances
Manage Client Interaction	Provide personal assistance (face to face)	Walk in Centre/Mobile office
	Provide telephonic assistance	Call Centre
	Provide assistance at employer (CLO) (Member/ Employer)	EGLS
	Manage Campaign (Member retirement)	CRM
	Outreach Programmes (Road Shows)	CRM
	Register Member for Self Service	CRM
	Resolve complaint	Complaints section
	Escalate quiry to relevent section/s	CRM
	Authenticate Client	CRM
	Perform Interaction	CRM
	Communicate Interaction Information	CRM
	conduct member education	CRM
	facilitate member retirement campaign	CRM
Manage inbound correspondence	Receive documents	OSS
	Linking documents	OSS
	Scanning documents	OSS
	Dispatch mails	OSS
	Indexing documents	OSS
Manage outbound correspondence	Response Client Email (Member, Pensioner,Beneficiary and 3rd Party)	NT and GEPF
	Send Letters (Member, Pensioner, Beneficiary and 3rd Party)	NT and GEPF (OSS)

	Send Information to Member and Pensioner on GEPF online	CRM and Communications
	Issue Benefits Statement	Membership
	Issue IRP5	Taxation
	Maintain Correspondence - GEPF	Pensioner Maintenance
Resolve Issue or Inquiry	Identify or Report Issue or Inquiry	CRM
	Classify, Investigate and Determine Cause	CRM
	Resolve Issue or Inquiry	CRM
	Notify Stakeholder(s)	CRM
	Prevent Recurrence	CRM
Prepare Statutory and Regulations Reports	Develop Performance Reporting (Monthly, Quarterly and Yearly)	M&E
	Publish APP Annual Report	Strategy
	Develop Customer Service Report	CRM
	Develop Employer Information Reporting	CRM
	Publish Strategic Plan	Strategy
	Compile National Credit Regulator Reports	GEPF funds
	Conduct Foreign Investments Reporting	GEPF funds
Manage Information	**Client/Pensioner**	
	Update member/pensioner details _NT	PMB (Post Medical Benefits)
	Update pensioner details - GEPF	Funeral Benefits
	Update pensioner details - GEPF	Pensioner Maintenance
	Maintain membership records of pensioners - GEPF	Pensioner Maintenance
	Maintain Client Information	Membership
	Perform Bank Verification - GEPF	Withdrawal
	Perform Bank Verification - NT	NT Funds
	Maintain banking details - GEPF	Membership
	Maintain banking details - NT	NT Funds
	Maintain contact details - GEPF	Membership
	Maintain contact details - NT	NT funds
	Maintain client life status (Perform auto life verification) - NT	NT Funds
	Maintain client life status (Perform auto life verification) - GEPF	Membership
	Maintain relationship information (incl. Nominations / Beneficiaries) - GEPF	Membership
	Maintain relationship information (incl. Nominations / Beneficiaries) - NT	NT Funds
	Employer	
	Maintain employer details - GEPF	CRM
	Maintain employer details - NT	NT Funds
	Member	
	Update member details - NT	IOD
	Update Member details - NT	Military Pensions
	Update member details - NT	Military Medical Account
	Update member details - NT	VIP
	Update member details - NT	Special Pensions

	Update member details - GEPF	Membership
	Maintain membership records of members - GEPF	Pensioner Maintenance
	Update TEPF member details - GEPF	TEPF Funds
	Update AIPF member details - GEPF	AIPF Funds
	Maintain Member - GEPF	Membership
	Maintain service periods	Membership
	Register Divorce	Membership
	Amend Service Years - GEPF, AIPF, TEPF	Pensioner Maintenance
	Amend service years - POS	Special Projects
	Amend service years - PDP - Active member and Pensioner	Special Projects
	Amend service years - Ciskei Strikers - Active member and Pensioner	Special Projects
	Amend service years - General Assistants - Active member and Pensioner	Special Projects
	Amend service years - NSF - Active member and Pensioner	Special Projects
	Manage pre-amalgamation period	Membership
	Contribution	
	Perform compulsory contribution accounting - PERSAL	Contributions
	Perform contribution accounting - Manual contributors	Contributions
	Perform POS Recon	Contributions
	Do additional liability recon	Contributions
	Perform voluntary contribution accounting - PERSAL	Contributions
	Transfer in	Membership
	Transfer out	Membership
	Maintain Estate Late information	Estate management
	Beneficiary	NT Funds
	Update beneficiary details - NT	IOD
	Update beneficiary details - NT	Military Pensions
	Update beneficiary details - NT	VIP
	Update beneficiary details - NT	Special Pensions
	Maintain spouse information	Pensioner Maintenance
	Maintain special pensioner information - NT	Special Pensions
	Maintain IOD beneficiary information - NT	IOD
	Maintain VIP beneficiary information - NT	VIP
	Maintain Medical Subsidy beneficiary information - NT	Medical Subsidy
	Maintain Military beneficiary information - NT	Military
	Maintain child beneficiary information - GEPF	Pensioner Maintenance
	Maintain Funeral benefit beneficiary information - GEPF	Funeral Benefits
	Maintain military medical beneficiary details - GEPF	Membership
	Product	

	Maintain Product Information - GEPF	GEPF funds
	Maintain Product Information - NT	NT funds
	Re-Issue pensioner card	Pensioner Maintenance
	Request Benefit Statement	Self Service
	Evidence	
	Process Evidence	CRM - Mainly OSS
	Manage external document storage	CRM - OSS - Registry
	Third Party	
	Update Supplier details (Service provider) - NT	Military Medical Account
	Receive Contributions	EB Contribution
	Reconcile Contributions	EB Contribution
	Load Contributions	EB Contribution
	Allocate Contributions	EB Contribution
	facilitate collection and reconciliation of contribution	EB Contribution
	Processing FinRecon (Electronic Contributors)	EB Contribution
	Processing manual Contribution billing	EB Contribution
	Processing purchase of Service Run (POS) Run reconciliation	EB Contribution
	Processing additional Liabilities;	EB Contribution
	Handle pensionable Salary confirmations, Contribution Queue.	EB Contribution
	Member	
	Capture Member (IOD)- NT	IOD
	Admit GEPF Member - GEPF	Membership
	Admit Post Medical Benefit Member - NT	Post Medical Benefits
	Admit military pensions member (injured or disable member) - NT	Military Pensions
	Admit VIP benefits member - NT	VIP
	Admit special pensions member - NT	Special Pensions
	Admit PDP member - GEPF	Special Projects
	Admit NSF member - GEPF	Special Projects
	Beneficiary	
	Capture Beneficiary details(IOD)- NT	IOD
	Admit Spouse (upon member's death) - NT	Military Pensions
	Admit Spouse(VIP)- NT	VIP
	Admit Orphan (VIP) - NT	VIP
	Admit beneficiary into special pensions (upon member's death) - NT	Special Pensions
	Admit Spouse Pension Benefits (upon member's death) - GEPF	Pensioner Maintenance
	Admit Child and Orphan Pension Benefits (upon member's death) - GEPF	Pensioner Maintenance
	Admit TEPF Spouse (upon member's death) - GEPF	TEPF fund
	Admit AIPF Spouse (upon member's death) GEPF	AIPF fund
Manage Client Interaction	Conduct customer Satisfaction Service	CRM
	Asses Customer Service Improvement	CRM
	Feedback Stakeholders	CRM

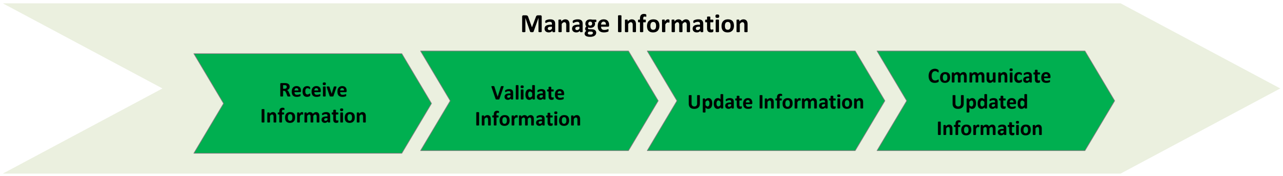
Create Financial Statements	Prepare and review general ledger reconciliations for National Treasury Funds	EB Finance
	Prepare annual financial statements of TEPF, AIPF and GEPF	EB Finance
	Prepare annual financial statements of National Treasury Funds	EB Finance
	Prepare reconciliation between CIVPEN and BAS entities - GEPF	GEPF funds
	Prepare reconciliation between CIVPEN and BAS entities - NT	NT funds
	Compile Fund Financial Statements	NT/GEPF
	Prepare and review general ledger reconciliations for TEPF, AIPF and GEPF	GEPF funds
	Create new general ledger account	EB Finance
Prepare Fund Reconcilliations	Recall payment made	EB Finance
	Payments and cancellation of post office transactions	EB Finance
	Allocate and deposit cash received	EB Finance
	Provide AIPF and TEPF provision on benefit payable	EB Finance
	Close bookkeeping month	EB Finance
	Manage monthly variances of GEPF benefits	GEPF funds
	Manage monthly variances NT benefits	NT Funds
	Calculate and authorise interest payments not calculated by the system	EB Finance
Manage Cash Flow	Prepare daily investments/disinvestment of funds to or from the PIC	Finance
	Capture and allocate other receipt from the bank statement	Finance
	Prepare monthly reconciliation of investments and disinvestments of funds to and from PIC and reporting to National Treasury and GEPF	Finance
	Prepare monthly bank reconciliations for GEPF, AIPF,TEPF and VOTE and reporting to National Treasury and GEPF	Finance
	Prepare monthly intercompany reconciliations and transfer thereof	Finance
Manage Investment accounting	Receive investment reports from external investment accountants	Finance
	Review investment reports	Finance
	Record monthly movement on CIVPEN	Finance
	Perform and review reconciliation of TB	Finance
	Review recon of external investment accountant, asset manager and PIC	Finance
	Pass PAIDF journals	Finance
	Conduct internal reporting on investments	Finance
	Prepare information for financial disclosure	Finance
	Conduct external reporting on investments	Finance
	Prepare annual financial statements for GEPF, AIPF and TEPF	Finance
Resolve Issue or Inquiry	Refer clients complaints	CRM
	handle client complaints	CRM
	Resolved client complaints	CRM

Manage Information Systems	Consolidate benefits stats	MIS
	publish MIS reports	MIS
	Develop SLA Reporting	MIS
	Compile Statistical Reports	MIS
Manage Service request	Provide client access	Information Security / BSS
	Provide user access	Information Security / BSS
	Facilitate Identity Access Management	BSS
	Facilitate Self Service Access	CRM/BSS
	Facilitate access to GPAA building	Physical Security
	Facilitate offices access	Physical Security
	Receive Client Access Request	CRM
	Authenticate Client	CRM
	Process Client Access Request	CRM
	Provide Access Rights	CRM
	Communicate Access Information	CRM
Provide Post retirement Support	facilitate outreach campaign	CRM
	Deliver Post-retirement Support	CRM
Manage Data (Manage enterprise data)	Develop analysis of exits cases	ICT
	Facilitate data arrangment	ICT
	Develop MIS reports	ICT
Manage Taxation	Facilitate tax certificate	Finance
	Facilitate tax reconciliation	Finance
	Facilitate tax directive	Finance
	Facilitate tax adjustment	Finance
	Develop taxation management reports	Finance

A mapping of the value stages and related processes of Core Business value stream and Administrative value stream, are unpacked below.

Value Stream: Manage Information

Value Stream:



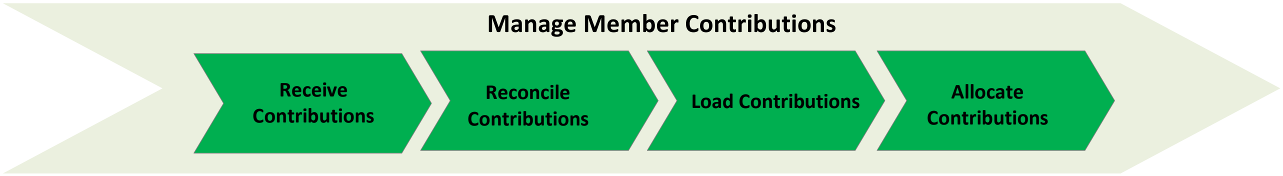
Value Stages and Processes:

Receive Information	**Validate Information**	**Update Information**	**Communicate (updated) Information**
Channel Operations	Capture Case Information	Capture Case Information	Channel Operations (L2)
Capture Case Information	Administer Client Information	Administer Client Information	Capture Case Information
Collect Evidence	Administer Member Information	Administer Member Information	Report Client Information
Associate Evidence	Administer Contribution Information	Administer Contribution Information	Report Member Information
Store Evidence	Administer Beneficiary Information	Administer Beneficiary Information	Report Contribution Information
Retrieve Evidence	Reconcile Contributions		Report Finance Information
Apply Case Routing Rule	Adjust Service Period	Adjust Service Period	
Process Work Queue Case	Administer Member Debt	Administer Member Debt	
Maintain Case State	Validate Payment Channel		

Report Client Information	Verify Evidence (Digital Signatures)		Report Evidence Information (L2)
Report Member Information	Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule
Report Contribution Information	Process Work Queue Case	Process Work Queue Case	Process Work Queue Case
Report Beneficiary Information	Escalate Case	Escalate Case	Escalate Case
Report Finance Information	Report Case State	Report Case State	Report Case State
Report Evidence Information	Measure Case Time	Measure Case Time	Measure Case Time
Report Case State	Maintain Case State	Maintain Case State	Maintain Case State
Escalate Case			
Measure Case Time			

Value Stream: Manage Member Contributions

Value Stream:

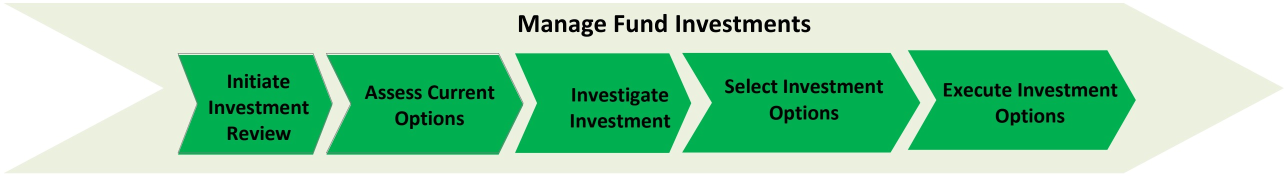


Value Stages and Processes:

Receive Contributions	Reconcile Contributions	Load Contributions	Allocate Contributions
Member Management (L1)	Member Management (L1)	Member Management (L1)	Member Management (L1)
Employer Management (L1)	Employer Management (L1)	Employer Management (L1)	Employer Management (L1)
Evidence Management (L1)	Finance Management (L1)	Finance Management (L1)	Finance Management (L1)
Finance Management (L1)			

Value Stream: Manage Fund Investments

Value Stream:

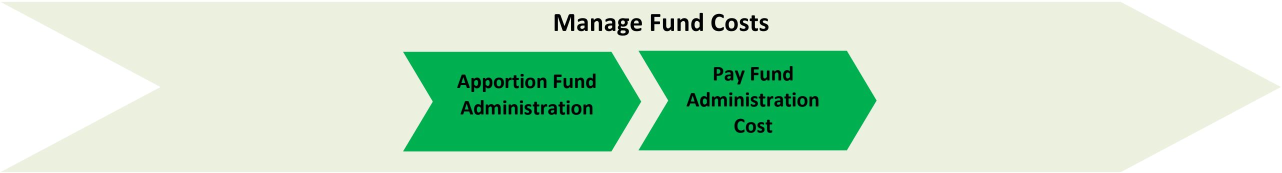

Manage Fund Investments
Initiate Investment Review
Assess Current Options
Investigate Investment
Select Investment Options
Execute Investment Options

Value Stages and Processes:

Initiate Investment Review	Assess Current Options	Investigate Investment Options	Select Investment Options	Execute Investment Options
Finance Management (L1)	Finance Management (L1)	Finance Management (L1)	Finance Management (L1)	Finance Management (L1)
Product Management (L1)	Product Management (L1)	Product Management (L1)	Product Management (L1)	Product Management (L1)

Value Stream: Manage Fund Costs

Value Stream:



Value Stages and Processes:

Apportion Fund Administration	**Pay Fund Administration Cost**
Finance Management (L1)	Finance Management (L1)
Product Management (L1)	Product Management (L1)

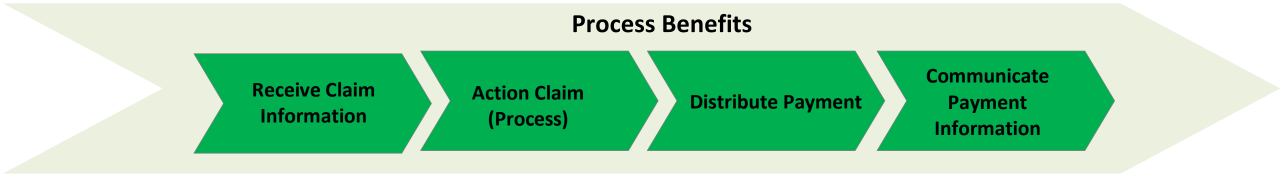
Additional Information

Current state

Requirements

Value Stream: Process Benefits

Value Stream:



Value Stages and Processes:

Receive Claim Information	Action Claim (Process)	Distribute Payment	Communicate Payment Information
Capture Case Information	Capture Case Information	Capture Case Information	Capture Case Information
Schedule Channel Operations	Validate Beneficiary		Channel Operations(L2)
Channel Availability	Calculate Benefit		Report Benefit Information
Collect Evidence	Administer Benefit information		
	Administer Member Debt		
	Beneficiary Administration (L2)	Beneficiary Administration (L2)	
Associate Evidence	Administer Beneficiary Information	Administer Beneficiary Information	
	Collect Evidence	Validate Payment Channel	
	Associate Evidence	Disburse Benefit	
Verify Evidence (Digital Signatures)	Verify Evidence (Digital Signatures)		
Store Evidence	Store Evidence		

Retrieve Evidence	Retrieve Evidence		
Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule
Process Work Queue Case	Process Work Queue Case	Process Work Queue Case	Process Work Queue Case
Maintain Case State	Maintain Case State	Maintain Case State	Maintain Case State
Report Client Information			
Report Member Information	Report Member Information	Report Member Information	
Report Contribution Information			
Report Beneficiary Information	Report Beneficiary Information	Report Beneficiary Information	Report Beneficiary Information
Report Finance Information	Report Finance Information	Report Finance Information	
Report Evidence Information	Report Evidence Information (L2)		
Report Case State	Report Case State	Report Case State	Report Case State
Escalate Case	Escalate Case	Escalate Case	Escalate Case
Measure Case Time	Measure Case Time	Measure Case Time	Measure Case Time

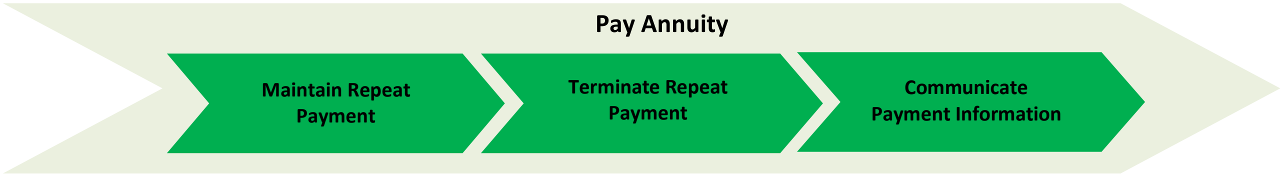
Additional Information

Current state

Requirements

Value Stream: Pay Annuity

Value Stream:



Value Stages and Processes:

Maintain Repeat **Payment**	**Terminate Repeat** **Payment**	**Communicate** **Payment Information**
(Capture Case Information)	*(Capture Case Information)*	Capture Case Information
(Administer Benefit information)	Administer Benefit information	Channel Operations(L2)
(Administer Beneficiary Information)	Administer Beneficiary Information	Report Benefit Information
Report Beneficiary Information	Report Beneficiary Information	Process Work Queue Case
Report Benefit Information	Report Benefit Information	Maintain Case State
(Validate Payment Channel)	*(Validate Payment Channel)*	Report Beneficiary Information
(Administer Payment Channel)	*(Administer Payment Channel)*	Apply Case Routing Rule
Disburse Benefit	Disburse Benefit	Process Work Queue Case
Report Case State	Report Case State	Report Case State
Escalate Case	Escalate Case	Escalate Case
Measure Case Time	Measure Case Time	Measure Case Time
	Report Client Information	
	(Administer Guardian)	*(Report Guardian Information)*
		Manage Channel Queue

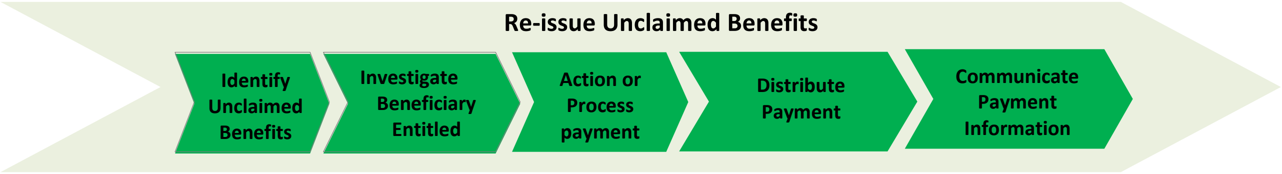
Additional Information

Current state

Requirements

Value Stream: Re-issue Unclaimed Benefits

Value Stream:


Re-issue Unclaimed Benefits
Identify Unclaimed Benefits
Investigate Beneficiary Entitled
Action or Process payment
Distribute Payment
Communicate Payment Information

Value Stages and Processes:

Identify Unclaimed Benefits	**Investigate Beneficiary Entitled**	**Action / Process payment**	**Distribute Payment**	**Communicate Payment Information**
Administer Unclaimed Inventory				
Locate Unclaimed Beneficiary				
Capture Case Information	Capture Case Information	Capture Case Information	Capture Case Information	Capture Case Information
Collect Evidence	Collect Evidence	Collect Evidence		
Associate Evidence	Associate Evidence	Associate Evidence		
Verify Evidence (Digital Signatures)	Verify Evidence (Digital Signatures)	Verify Evidence (Digital Signatures)		
Store Evidence	Store Evidence	Store Evidence		
Retrieve Evidence	Retrieve Evidence	Retrieve Evidence		
Report Evidence Information	Report Evidence Information	Report Evidence Information	Report Evidence Information	Report Evidence Information

Maintain Case State	Maintain Case State	Maintain Case State	Maintain Case State	Maintain Case State
Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule
Process Work Queue Case	Process Work Queue Case	Process Work Queue Case	Process Work Queue Case	Process Work Queue Case
Administer Client Information	Administer Client Information	*(Validate Payment Channel)*		
Report Client Information	Report Client Information	*(Administer Payment Channel)*		
(Administer Member Information)	*(Administer Member Information)*	*(Administer Member Information)*		
Report Member Information	Report Member Information	Report Member Information	Report Member Information	Report Member Information
		(Administer Benefit Information)		
Report Benefit Information	Report Benefit Information	Report Benefit Information	Report Benefit Information	Report Benefit Information
	Administer Beneficiary Information	Administer Beneficiary Information		
Report Beneficiary Information	Report Beneficiary Information	Report Beneficiary Information	Report Beneficiary Information	Report Beneficiary Information
	(Administer Guardian)	*(Administer Guardian)*		
	(Report Guardian Information)	*(Report Guardian Information)*	*(Report Guardian Information)*	*(Report Guardian Information)*
		Disburse Benefit	Disburse Benefit	

Report Finance Information	Report Finance Information	Report Finance Information	Report Finance Information	Report Finance Information
Report Case State	Report Case State	Report Case State	Report Case State	Report Case State
Escalate Case	Escalate Case	Escalate Case	Escalate Case	Escalate Case
Measure Case Time	Measure Case Time	Measure Case Time	Measure Case Time	Measure Case Time
			Manage Tax	Manage Channel Queue

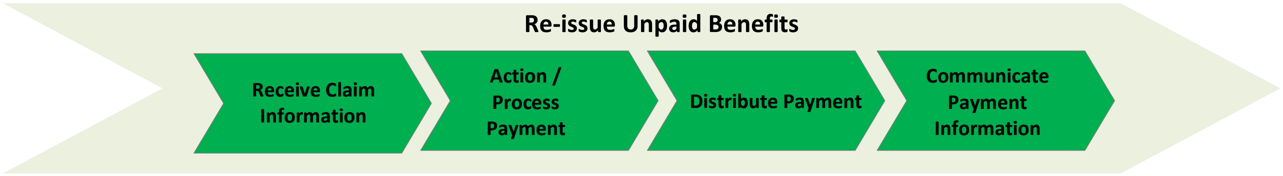
Additional Information

Current state

Requirements

Value Stream: Re-issue Unpaid Benefits

Value Stream:



Value Stages and Processes:

Identify Unpaid Benefits	**Action / Process Payment**	**Distribute Payment**	**Communicate Payment Information**
Client Management (L1)	*Client Management (L1)*	*Client Management (L1)*	*Client Management (L1)*
Benefit Claim Management (L1)	*Benefit Claim Management (L1)*	*Benefit Management (L1)*	*Benefit Claim Management (L1)*
Case Management (L1)	*Case Management (L1)*	*Finance Management (L1)*	
Administer Unpaid Inventory			
Locate Unpaid Beneficiary			
Capture Case Information	Capture Case Information	Capture Case Information	Capture Case Information
Collect Evidence	Collect Evidence		
Associate Evidence	Associate Evidence		
Verify Evidence (Digital Signatures)	Verify Evidence (Digital Signatures)		
Store Evidence	Store Evidence		
Retrieve Evidence	Retrieve Evidence		
Report Evidence Information	Report Evidence Information	Report Evidence Information	Report Evidence Information

Maintain Case State	Maintain Case State	Maintain Case State	Maintain Case State
Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule
Process Work Queue Case	Process Work Queue Case	Process Work Queue Case	Process Work Queue Case
Administer Client Information	*Administer Client Information*		
Report Client Information	Report Client Information		
(Administer Member Information)	*(Administer Member Information)*		
Report Member Information	Report Member Information	Report Member Information	Report Member Information
Report Benefit Information	Report Benefit Information	Report Benefit Information	Report Benefit Information
	Administer Beneficiary Information		
Report Beneficiary Information	Report Beneficiary Information	Report Beneficiary Information	Report Beneficiary Information
	(Administer Guardian)		
	(Report Guardian Information)	*(Report Guardian Information)*	*(Report Guardian Information)*
		Disburse Benefit	
Report Finance Information	*Report Finance Information*	Report Finance Information	Report Finance Information
Report Case State	Report Case State	Report Case State	Report Case State
Escalate Case	Escalate Case	Escalate Case	Escalate Case
Measure Case Time	Measure Case Time	Measure Case Time	Measure Case Time
		Manage Tax	Manage Channel Queue

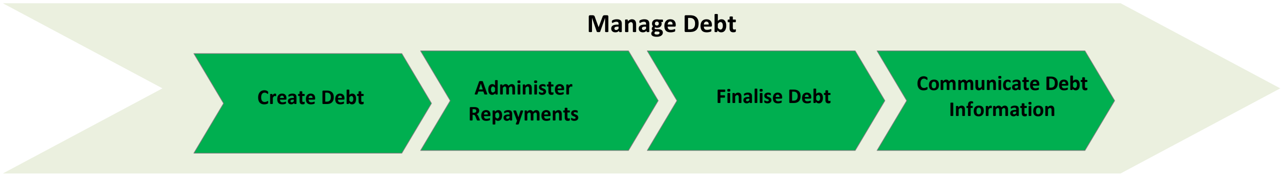
Additional Information

Current state

Requirements

Value Stream: Manage Debt

Value Stream:



Value Stages and Processes:

Create Debt	**Administer Repayments**	**Finalise Debt**	**Communicate Debt Information**
Case Management (L1)	*Case Management (L1)*	*Case Management (L1)*	Capture Case Information
Maintain Case State	Maintain Case State	Maintain Case State	Maintain Case State
Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule
Process Work Queue Case	Process Work Queue Case	Process Work Queue Case	Process Work Queue Case
(Administer Client Information)	Administer Contribution Information	Administer Contribution Information	Report Debt Information
(Report Client Information)	Report Contribution Information	Report Contribution Information	Report Member Information
Administer Member Information	Administer Member Information	Administer Member Information	Report Finance Information
Report Member Information	Report Member Information	Report Member Information	Report Case State
Administer Debt Information	Administer Debt Information	Administer Debt Information	Escalate Case
Report Debt Information	Report Debt Information	Report Debt Information	Measure Case Time

Administer Finance Information	*Administer Finance Information*	*Administer Finance Information*	Manage Channel Queue
Report Finance Information	*Report Finance Information*	*Report Finance Information*	
Collect Evidence	Collect Evidence	Collect Evidence	
Associate Evidence	Associate Evidence	Associate Evidence	
Verify Evidence (Digital Signatures)	Verify Evidence (Digital Signatures)	Verify Evidence (Digital Signatures)	
Store Evidence	Store Evidence	Store Evidence	
Retrieve Evidence	Retrieve Evidence	Retrieve Evidence	
Report Evidence Information	Report Evidence Information	Report Evidence Information	
Report Case State	Report Case State	Report Case State	
Escalate Case	Escalate Case	Escalate Case	
Measure Case Time	Measure Case Time	Measure Case Time	

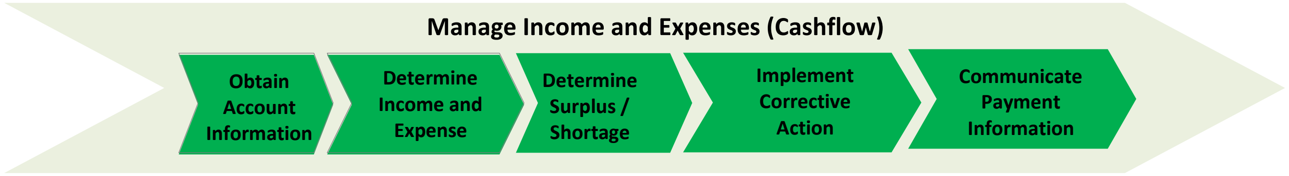
Additional Information

Current state

Requirements

Value Stream: Manage Income and Expenses (Cashflow)

Value Stream:


Manage Income and Expenses (Cashflow)
Obtain Account Information
Determine Income and Expense
Determine Surplus / Shortage
Implement Corrective Action
Communicate Payment Information

Value Stages and Processes:

Obtain Account Information	Determine Income and Expense	Determine Surplus/ Shortage	Implement Corrective Action	Communicate Payment Information
Manage Channel Availability				Manage Channel Availability
Manage Channel Queue	Accounts Payable Accounting			
	Accounts Receivable Accounting			
Manage Data Operations	Manage Data Operations	Manage Data Operations		
	Administer Finance Information	Administer Finance Information	Administer Finance Information	
	Report Finance Information	Report Finance Information	Report Finance Information	Report Financial information
	General Ledger Accounting	General Ledger Accounting	General Ledger Accounting	
	Manage Financial Accounts	Manage Financial Accounts	Manage Financial Accounts	

			Manage Funds	
			Financial Provisioning	
				Manage Channel Operations (L2)
				Manage Channel Queue

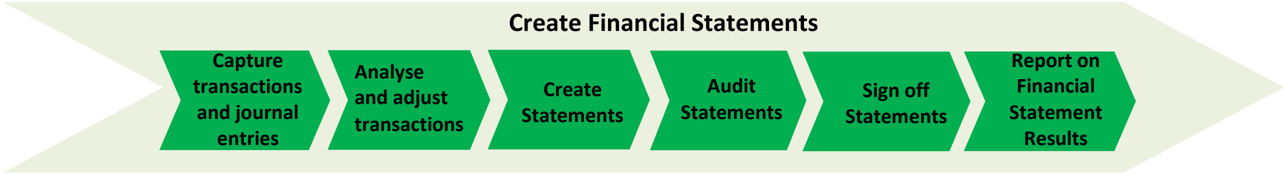
Additional Information

Current state

Requirements

Value Stream: Create Financial Statements

Value Stream:


Create Financial Statements
Capture transactions and journal entries
Analyse and adjust transactions
Create Statements
Audit Statements
Sign off Statements
Report on Financial Statement Results

Value Stages and Processes:

Capture Transactions and Journal Entries	**Analyse and Adjust Transactions**	**Create Statements**	**Audit Statements**	**Sign off Statements**	**Report on Financial Statement Results**
Finance Matching	Finance Matching	Administer Debt Information		Perform case routing	
Manage Financial Accounting	Financial Governance	Financial Governance	Financial Governance	Financial Governance	
		Report Finance Information	Report Finance Information	Report Finance Information	Report Finance Information
			Report Debt Information		Report Debt Information

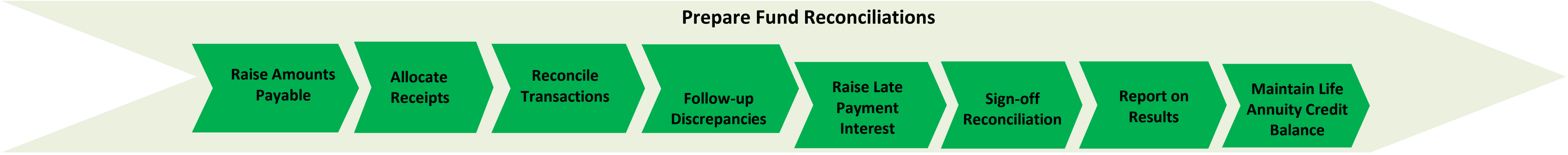
Additional Information

Current state

Requirements

Value Stream: Prepare Fund Reconciliations

Value Stream:



Value Stages and Processes:

Raise Amounts Payable	Allocate Receipts	Reconcile Transactions	Follow-up Discrepancies	Raise Late Payment Interest	Sign-off Reconciliation	Report on Results	Maintain Life Annuity Credit Balance
Report Debt Information	Financial Matching	Reconcile Debts		Perform Debt Administration			
		Report Debt Information	Report Debt Information	Report Debt Information			
				Report Finance Information			
				Channel Operations (L2)			Perform Debt Administration

					Financial Governance	Report Finance Information	Report Finance Information
					Route Case	Report Debt Information	Report Debt Information

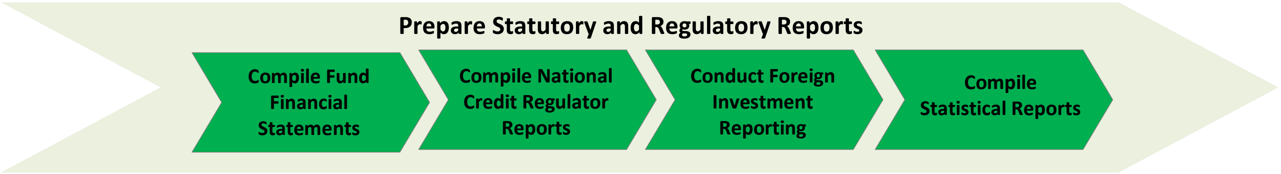
Additional Information

Current state

Requirements

Value Stream: Prepare Statutory and Regulatory Reports

Value Stream:

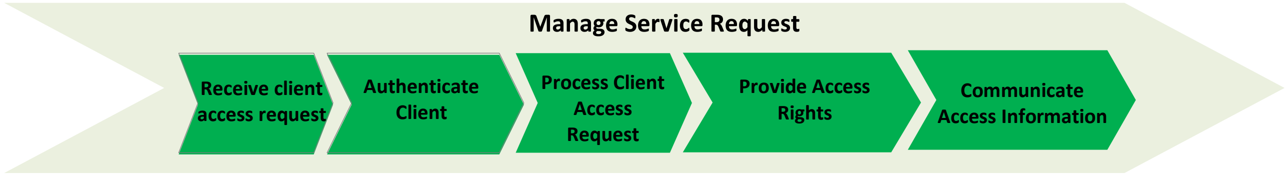

Prepare Statutory and Regulatory Reports
Compile Fund Financial Statements
Compile National Credit Regulator Reports
Conduct Foreign Investment Reporting
Compile Statistical Reports

Value Stages and Processes:

Compile Fund Financial Statements	Compile National Credit Regulator Reports	Conduct Foreign Investment Reporting	Compile Statistical Reports
Finance Management (L1)	Finance Management (L1)	Finance Management (L1)	Finance Management (L1)
Debt Management (L1)			

Value Stream: Manage Service Request

Value Stream:


Manage Service Request
Receive client access request
Authenticate Client
Process Client Access Request
Provide Access Rights
Communicate Access Information

Value Stages and Processes:

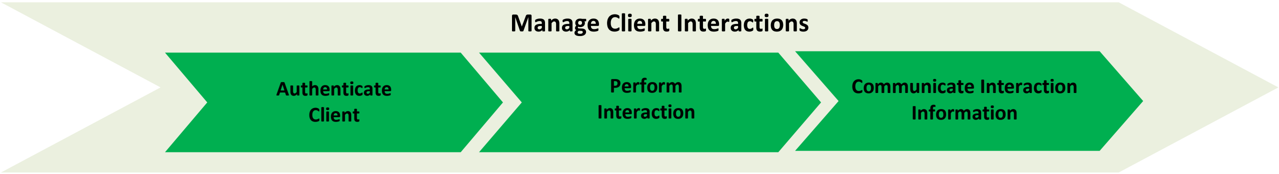
Receive Client Access Request	**Authenticate Client**	**Process Client Access Request**	**Provide Access Rights**	**Communicate Access Information**
	Case Management (L1)			Client Experience Management
	Service Channel Management (L1)		(Maintain User Role)	
	Evidence Management (L1)			
Control Client Access		Control Client Access	Control Client Access	
Manage Channel Availability	Manage Channel Availability	Manage Channel Availability	Manage Channel Availability	Manage Channel Availability
Manage Channel Queue	Manage Channel Queue	Manage Channel Queue	Manage Channel Queue	Manage Channel Queue
Schedule Channel Operations	Schedule Channel Operations	Schedule Channel Operations		Schedule Channel Operations

Capture Case Information		Capture Case Information	Capture Case Information	Capture Case Information
Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule
Process Work Queue Case	Process Work Queue Case	Process Work Queue Case	Process Work Queue Case	Process Work Queue Case
Collect Evidence	Collect Evidence	Collect Evidence		
Associate Evidence	Associate Evidence	Associate Evidence		
Verify Evidence (Digital Signatures)	Verify Evidence (Digital Signatures)	Verify Evidence (Digital Signatures)		
Store Evidence	Store Evidence	Store Evidence		
Retrieve Evidence	Retrieve Evidence	Retrieve Evidence		
Report Evidence Information	Report Evidence Information	Report Evidence Information		
Administer Client Information	Administer Client Information	Administer Client Information	Administer Client Information	Administer Client Information
		Administer Client Enquiry		
		Administer Client Complaint		
Report Client Information	Report Client Information	Report Client Information	Report Client Information	Report Client Information
(Administer Member Information)	*(Administer Member Information)*	*(Administer Member Information)*		

Report Member Information	*(Report Member Information)*	Report Member Information		
Maintain Case State	Maintain Case State	Maintain Case State	Maintain Case State	Maintain Case State
Escalate Case	Escalate Case	Escalate Case	Escalate Case	Escalate Case
Report Case State	Report Case State	Report Case State	Report Case State	Report Case State
Measure Case Time	Measure Case Time	Measure Case Time	Measure Case Time	Measure Case Time
Report Case Information	Report Case Information	Report Case Information	Report Case Information	Report Case Information
		(Administer Beneficiary Information)		
		(Report Beneficiary Information)		*(Report Beneficiary Information)*

Value Stream: Manage Client Interactions

Value Stream:


Manage Client Interactions
Authenticate Client
Perform Interaction
Communicate Interaction Information

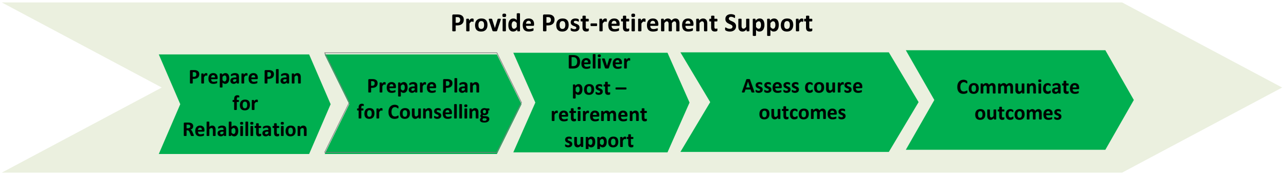
Value Stages and Processes:

Authenticate Client	Perform Interaction	Communicate Interaction Information
Case Management (L1)		Client Experience Management
Service Channel Management (L1)		
Evidence Management (L1)	Control Client Access	
Control Client Access	Manage Channel Availability	Manage Channel Availability
Manage Channel Availability	Manage Channel Queue	Manage Channel Queue
Manage Channel Queue	Schedule Channel Operations	Schedule Channel Operations
Schedule Channel Operations	Capture Case Information	Capture Case Information
Apply Case Routing Rule	Apply Case Routing Rule	Apply Case Routing Rule
Process Work Queue Case	Process Work Queue Case	Process Work Queue Case
Administer Client Information	Collect Evidence	
Report Client Information	Associate Evidence	
Maintain Case State	Verify Evidence (Digital Signatures)	
Escalate Case	Store Evidence	

Report Case State	Retrieve Evidence	
Measure Case Time	Report Evidence Information	Report Evidence Information
Report Case Information	Administer Client Information	Administer Client Information
	Administer Client Enquiry	
	Administer Client Complaint	
	Report Client Information	Report Client Information
	(Administer Member Information)	
	Report Member Information	*(Report Member Information)*
	Maintain Case State	Maintain Case State
	Escalate Case	Escalate Case
	Report Case State	Report Case State
	Measure Case Time	Measure Case Time
	Report Case Information	Report Case Information
	(Administer Beneficiary Information)	
	(Report Beneficiary Information)	*(Report Beneficiary Information)*
	(Report Contribution Information)	*(Report Contribution Information)*
	(Calculate Benefit)	
	(Report Debt Information)	*(Report Debt Information)*
	(Validate Payment Channel)	

Value Stream: Provide Post-retirement Support

Value Stream:

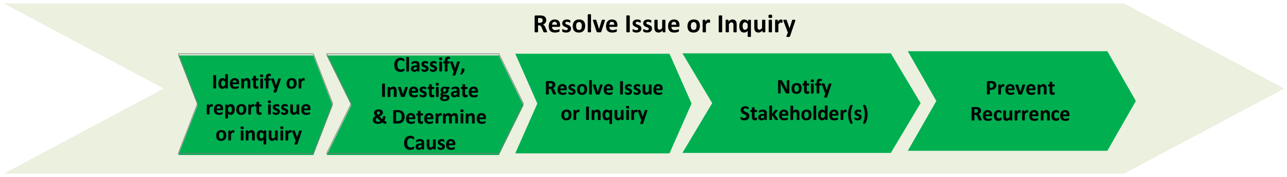

Provide Post-retirement Support
Prepare Plan for Rehabilitation
Prepare Plan for Counselling
Deliver post – retirement support
Assess course outcomes
Communicate outcomes

Value Stages and Processes:

Prepare Plan for Rehabilitation	Prepare Plan for Counselling	Deliver post-retirement support	Assess course outcomes	Communicate outcomes
Client Management (L1)	Client Management (L1)	Client Management (L1)	Client Management (L1)	Client Management (L1)
Member Management (L1)	Member Management (L1)	Member Management (L1)	Member Management (L1)	Member Management (L1)

Value Stream: Resolve Issue or Inquiry

Value Stream:



Value Stages and Processes:

Identify or Report Issue or Inquiry	**Classify, Investigate & Determine Cause**	**Resolve Issue or Inquiry**	**Notify Stakeholder(s)**	**Prevent Recurrence**
Service Channel Management (L1)		Service Channel Management (L1)	Service Channel Management (L1)	
Case Management (L1)	Case Management (L1)	Case Management (L1)	Case Management (L1)	
Client Management (L1)			Client Management (L1)	Client Management (L1)
Evidence Management (L1)	Evidence Management (L1)	Evidence Management (L1)		
				Enterprise Data Management (L1)

3.1.13 GPAA Information Foundation

In the context of Enterprise Architecture (EA), an Information Map is a visual representation or diagram that illustrates how data and information flow within an organization.

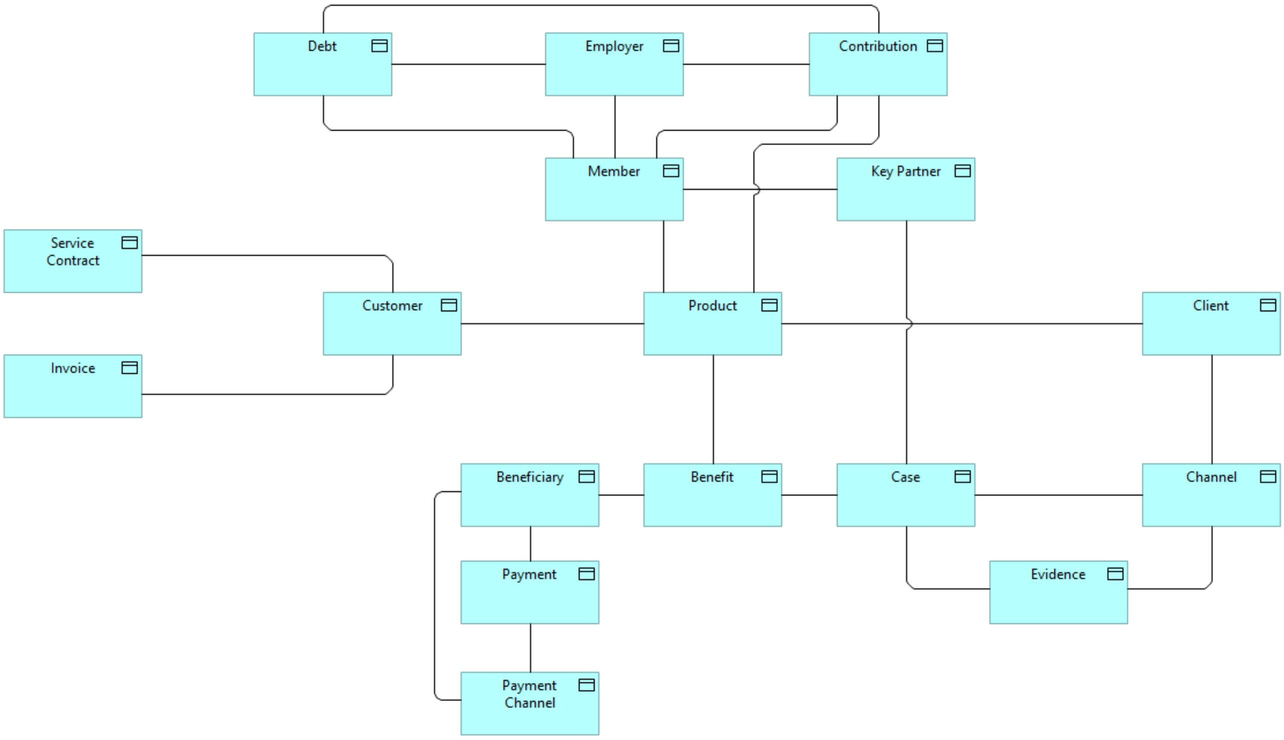


Figure 13 GPAA Information Map

The figure above depicts the information map of GPAA. This information map provides the business vocabulary that enables effective communication within GPAA.

The table below explains these relationships.

Information	Definition
Beneficiary	A person who has received or is still receiving the benefits after application of the product rules
Benefit	The actual monetary value that a beneficiary is entitled to as a result of applied product rules
Case	A formal request triggered by a client executed by a predefined set of actions sequenced and tracked with the purpose of fulfilling a formal request within a predetermined time frame

Channel	A communication route for communication from and to our clients, members and beneficiaries
Client	Any entity who interacts with the Administrator in his own capacity or on behalf of another person
Contribution	A payment for the purpose of building a fund for a specific purpose
Customer	An organisation on whose behalf the Administrator (GPAA) administers its benefits
Debt	A sum of money that is owed because of the various debt payment arrangements between a member, employer and the GPAA
Employer	An organisation that employs the member and usually is responsible for paying the contribution
Evidence	Tagged images or structured data representations submitted to the Administrator as proof to validate information
Key Partner	Organisations that the Administrator is dependent on so that services are delivered effectively and efficiently
Member	A person who has been admitted to a fund and is entitled to benefits as described in the product rules
Role	An organized group of people within GPAA with a particular purpose
Operational Finance	The management of money flowing into and out of bank accounts
Payment	The actual benefit of a recipient that is paid into a specific bank account
Payment Channel	A payment route to enable payment to our beneficiaries
Product	A set of rules that define the eligibility (conditions of receipt) of an individual and potential benefit(s) (calculation formula) that a product must provide to this individual in the occurrence of life events as described in said rules

Table: GPAA Information elements

3.1.14 Gaps, Findings & Considerations

The following factors for consideration have been defined based on analysis of the current business architecture assessment. These have been consolidated from various consultations and previous reviews. The Considerations column suggests how the findings can be resolved or approached.

Aspect	Findings	Considerations
Organisational Structure	• Structure is not fully aligned to strategy - the structure lacks Modernisation representation at the executive level. • Lack of flexibility of the structure and inability to attract and retain the right skills. • The form restricts how easily the structure can be amended to retain and acquire new skills, to make provision for additional roles in accordance with the strategy of the organisation.	The GPAA's structure should be designed to allow for better communication, decision-making, and problem-solving.
Processes	• Processes are still largely manual and paper based with duplication of efforts. • The GPAA is aware of which processes to optimise to improve client centricity. • Lack of adherence to the standard procedures with inconsistent exit /withdrawal processing requirements. • Manual processes have led to the duplication of efforts and inadequate monitoring controls: • There is a lack of urgency to optimise and automate processes as well as replacing legacy systems which results in long turnaround-times, missed SLA targets, and dissatisfied clients.	Business Process redesign is crucial. Process redesign and optimization is part of the Modernisation Programme's mandate. This is planned.
Performance monitoring and evaluation	• Performance management does not enforce consequence management. • While good performance processes exist, there is a poor performance culture within the organisation that does not enforce accountability and ownership, with an inadequate value proposition for employees to outperform and take ownership.	Establish a system for monitoring and evaluating the performance of the decentralised functions to identify any issues and make necessary adjustments.

Communication and coordination		Effective communication and coordination are critical for ensuring that the different parts of the organisation are working together effectively.
Staffing and Training	• Senior management lack industry specific capabilities such as finance, accounting, IT and actuarial science.	The GPAA will need to have the right staff in place to manage the new decentralised functions. Staff will need to be trained on new processes, procedures, and technologies including fraud detection.
Modernization	• No strategic direction for Modernisation • There is a lack of capacitation at an executive level to drive Modernisation and ensure there is a clearly defined and documented strategy and execution plan, to meet expectations for modernisation.	Capacitation through the Modernisation Programme
Client-Centricity	• Not well geared towards superior client-centricity • GPAA's client value proposition has a lack of value-add services, such as financial advisory, personalised communication and counselling offered to clients. Centralised functions affect how well clients are served with client-facing centres operating as regional touchpoints. Call-centres and digital offerings exist but are a point of frustration.	Business & Operating Model review to consider offering value-add services, such as financial advisory, personalised communication and counselling offered to clients.
Change Management	• Change management is not embedded within business operations. • Change management is not viewed as a strategic enabler and is not embedded within day-to-day operations, resulting in resistance to change, inadequate buy-in and adoption of new processes and systems.	To incorporate EA Modeling and use for Change Management and planning to depict the impact. Effective communication and coordination are critical for ensuring that the different parts of the organisation are working together effectively.
Reporting	• Lack of strategic reporting • The GPAA is good at producing reports and data but lacks the ability to turn data into insights through enhance business intelligence reports and dashboarding. This results in a lack of strategic insights	Leverage data analytics and associated tools for insights.

	and planning towards improving client experience.	
Operating Model	• Lack of formal processes to enforce accountability on employer departments. • There is no enforcement of the memorandum of understanding between the GPAA and employer departments to ensure accountability. This leads to lack of ownership and poor quality of data. Recent efforts over the past two months are bridging the gap on a better way of working with employer departments and issue resolution.	Define relevant processes, SOPs, SLA's, and Performance Measurement for employer engagement.

3.1.15 Modernisation Programme Requirements

The following Business Requirements have been defined for the programme.

Programme 2.1 Business Requirements

To reduce unnecessary delay time and repetitive tasks and ultimately to reduce the turnaround time, the Modernisation Programme solution must enable the workstreams comprising the following capabilities and value stream stages.

Capability	Value stream stage	Description
Member Information Management		The ability to maintain and manage all membership. information for purposes of administration from the start to the end of the membership.
	Receive Information	The activities required to receive information from specified sources and have it available to GPAA systems for validation.
	Validate information	The activities required to ensure that all received information is correct and complete.
	Update information	These are the activities required to make the correct information available to the GPAA database.
	Communicate information	The activities required to inform the stakeholder of the information maintenance outcome.
Contributions Management		The ability to process contributions towards membership.
	Receive contributions	The activities required to obtain contributions from members.
	Reconcile contributions	The activities required to determine whether the amounts received are the same as the amounts expected by the member.
	Load contributions	The activities required to record the correct contributions on the system.
	Allocate contributions	Activities related to the allocating a portion of their contributions to the fund and other housing home loan by the fund.

Capability	Value stream stage	Description
Benefit Payment		The ability to pay the correct benefit to the correct beneficiary.
	Receive Claim Information	The activities required to receive information from specified sources and have it available to GPAA systems for validation.
	Action Claim (Process)	The activities required to ensure that all received information is correct and complete.
	Disburse Payment	The activities required to pay the benefit to the beneficiary.
	Communicate Payment Information	The activities required to inform the stakeholder of the information maintenance outcome.
Benefit Disbursement Management		The ability to pay correct repeat payments to the correct beneficiary until the end condition occurs.
	Maintain repeat payment	Activities required to ensure that the annuity payment is paid correctly and on time.
	Terminate repeat payment	Activities required to stop the repeat payment if the end conditions occur.
	Communicate payment information	Activities required to make available all required payment information to all stakeholders.
Service Request Management		The ability to correctly determine the identity of a client and provide credentials to a client for the purpose of using a GPAA systems.
	Receive Client access request	The activities involved to ensure that relevant, complete, and correct information for service request purposes is received.
	Process client access request	The activities required to determine whether the requesting client is allowed to receive required information according to client access control rules.
	Provide access rights	The activities required to enable the requesting client to receive the allowed access.
	Communicate access information	The activities required to inform stakeholders of the result of the access request.

Capability	Value stream stage	Description
Post Retirement Support Provision		The ability to support pensioners post-retirement with services to reduce the risk of loneliness and social isolation and eventually premature death.
	Prepare Plan for Rehabilitation	The activities required to gather all inputs for planning of the support.
	Prepare Plan for Rehabilitation	The activities required as inputs to establish counselling.
	Deliver post-retirement support	The activities involved to deliver the support from the start up to the end of the course.
	Assess course outcomes	The activities required to do periodic assessment against agreed course outcomes.
	Communicate outcomes	The activities required to communicate course outcomes with stakeholders utilizing multiple communication channels.

Programme 2.2 Requirements

The scope of this documentation is limited to the following capabilities of the GEPF funds:

Capability	**Description**
Member Information Management	The ability to maintain and manage all membership information for purposes of administration from the start to the end of the membership.
Contributions Management	The ability to process contributions towards membership.
Benefit Payment	The ability to pay the correct benefit to the correct beneficiary.
Benefit Disbursement Management	The ability to pay correct repeat payments to the correct beneficiary until the end condition occurs.
Service Request Management	The ability to correctly determine the identity of a client and provide credentials to a client for the purpose of using the GPAA systems.
Post Retirement Support Provision	The ability to support pensioners post-retirement with services to reduce the risk of loneliness and social isolation and eventually premature death.
Enterprise Data Management	The ability to plan, execute on and oversee policies, practices and projects that acquire, control, protect, deliver, and enhance the value of information and data assets.

The requirements must fall under any of the abovementioned capabilities. Some of the requirements are for the capabilities that were never modernized before and therefore new to Modernisation for enablement. Others are for capabilities that are already modernized and therefore they need enhancement. The business requirements are classified as new to Modernisation requirements or continuous improvement requirements.

FMS

Business Capabilities and Value Streams

Capability	Value Streams	Description
Financial Management	Funds Management	The ability to manage cash collections and disbursements made by the Administrator and, when appropriate, to transfer cash from those units to parent-level bank accounts managed by the government's treasury unit.
	Cashflow management	The ability to forecast and manage cash inflows, outflows, and cash balances to ensure adequate liquidity.
	Bank Account Information Management	The ability to view the treasury bank accounts by assessing the cash that flows in and out of the bank accounts.
	Treasury Accounting	The ability to ensure that all treasury financial transactions are accounted for and reported on in the administrator's financial records.
	General ledger Accounting	The ability to collect, account and record all the financial transactions on GPAA's assets, liabilities, equity, expenses and income on their ledgers according to the accounting model.
	Statutory Reporting	The ability for GPAA to follow processes to submit financial and non-financial information to government agencies according to the laws and regulations applicable to an administrator.
	Finance Reconciliation	The ability for GPAA to compare two different data sets to verify that the information within them is accurate.
	Tax management	The ability for GPAA to comply with tax laws and regulations
	Financial Governance	

Customer Relationship Management (CRM) Business Requirements

To reduce unnecessary delay time and repetitive tasks and ultimately to reduce the turnaround time, the Modernisation Programme solution must enable the workstreams comprising the following capabilities and value stream stages.

Capability	Value Stream Stage	Description
Client Interaction		The ability to receive, resolve and report back on questions received from clients via all channels.
	Authenticate client	The activities involved in verifying the caller, or walk-in client in order to avoid disclosing confidential information to the wrong person.
	Perform interaction	The activities required to receive, resolve, as well as report back on the questions received from clients via all channels.
	Communicate interaction information	The activities involved in providing feedback regarding client interaction.
	Communicate access information	The activities required to inform stakeholders of the result of the access request.
Client Information Management		The ability to receive, resolve and report back on questions received from clients via all channels.
	Receive Information	The activities involved in verifying the caller, or walk-in client in order to avoid disclosing confidential information to the wrong person.
	Receive Information	The activities required to receive ana validate information submitted to GPAA by the member or employer
	Update Information	The activities required to capture information from the employer or the member after the source documentation has been validated.
	Communicate Updated Information	The activities required to inform stakeholders of the updates made to their record.
Post Retirement Support Provision		The ability to support pensioners post-retirement with services to reduce the risk of loneliness and social isolation and eventually premature death.
	Prepare Plan for Rehabilitation	The activities required to gather all inputs for planning of the support.

Capability	Value Stream Stage	Description
	Prepare Plan for Rehabilitation	The activities required as inputs to establish counselling.
	Deliver post-retirement support	The activities involved to deliver the support from the start up to the end of the course.
	Assess course outcomes	The activities required to do periodic assessment against agreed course outcomes.
	Communicate outcomes	The activities required to communicate course outcomes with stakeholders utilizing multiple communication channels.

Financial Management System (FMS) Requirements

GPAA seeks to procure and implement a powerful, well integrated financial management system.

FMS Business Capabilities and Value Streams

Capability	Value Streams	Description
Financial Management	Funds Management	The ability to manage cash collections and disbursements made by the Administrator and, when appropriate, to transfer cash from those units to parent-level bank accounts managed by the government's treasury unit.
	Cashflow management	The ability to forecast and manage cash inflows, outflows, and cash balances to ensure adequate liquidity.
	Bank Account Information Management	The ability to view the treasury bank accounts by assessing the cash that flows in and out of the bank accounts.
	Treasury Accounting	The ability to ensure that all treasury financial transactions are accounted for and reported on in the administrator's financial records.
	General ledger Accounting	The ability to collect, account and record all the financial transactions on GPAA's assets, liabilities,

Capability	Value Streams	Description
		equity, expenses and income on their ledgers according to the accounting model.
	Statutory Reporting	The ability for GPAA to follow processes to submit financial and non-financial information to government agencies according to the laws and regulations applicable to an administrator.
	Finance Reconciliation	The ability for GPAA to compare two different data sets to verify that the information within them is accurate.
	Tax management	The ability for GPAA to comply with tax laws and regulations
	Financial Governance	The ability for GPAA to collect, manage, monitors and control financial information.

4 Data Architecture

Data plays a critical role in GPAA's ability to carry out its mandate.

GPAA must hold the right data about its clients, its partners, the funds that it administers and other entities.

4.1.1 Key Data Entities

GPAA has a wide range of data entities to manage its operations.

This diagram is the information map for GPAA Core Business.

It depicts the key data objects and association with some of the key Business Architecture roles and objects (in yellow) to provide context into the data architecture.

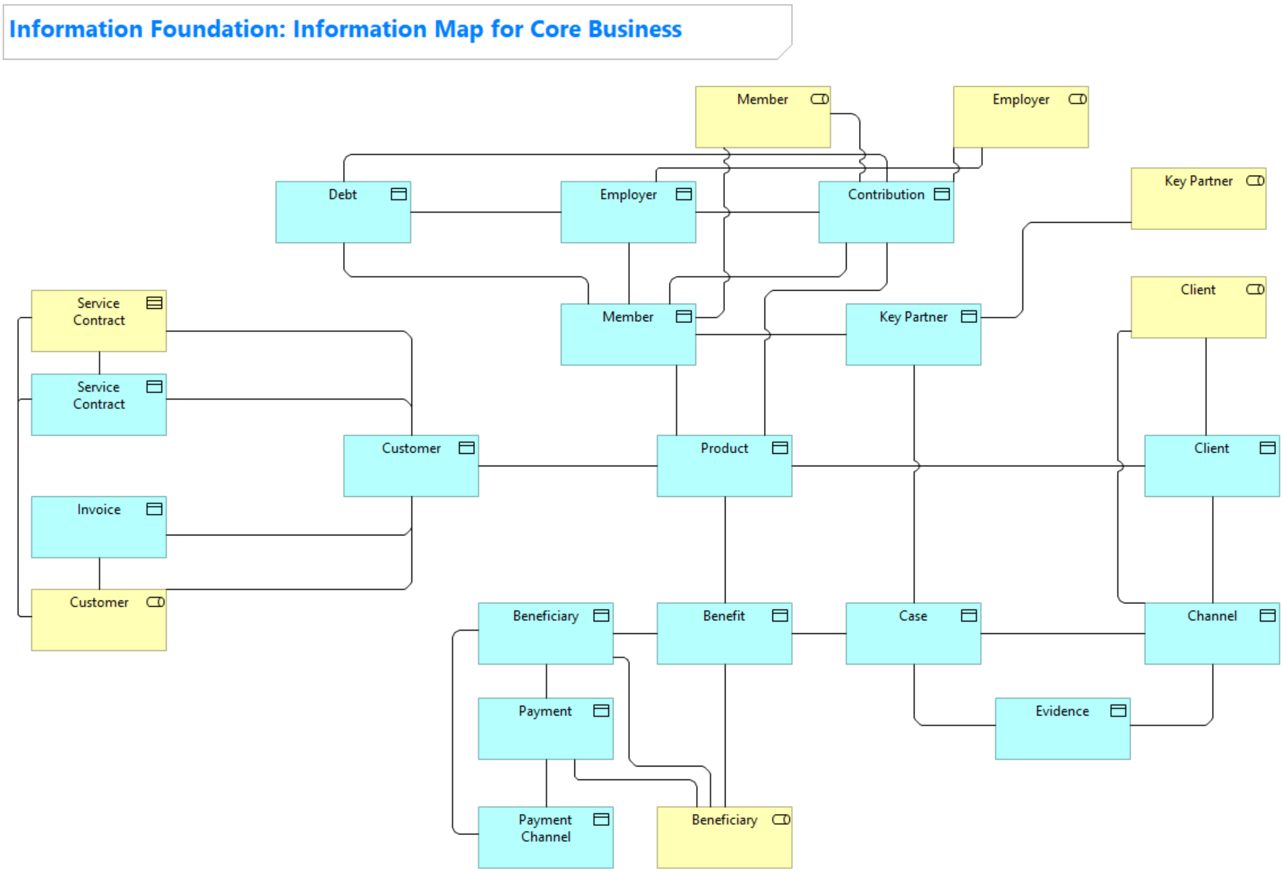


Figure 14 Information map for GPAA Core Business

Below is a broad categorization of data entities:

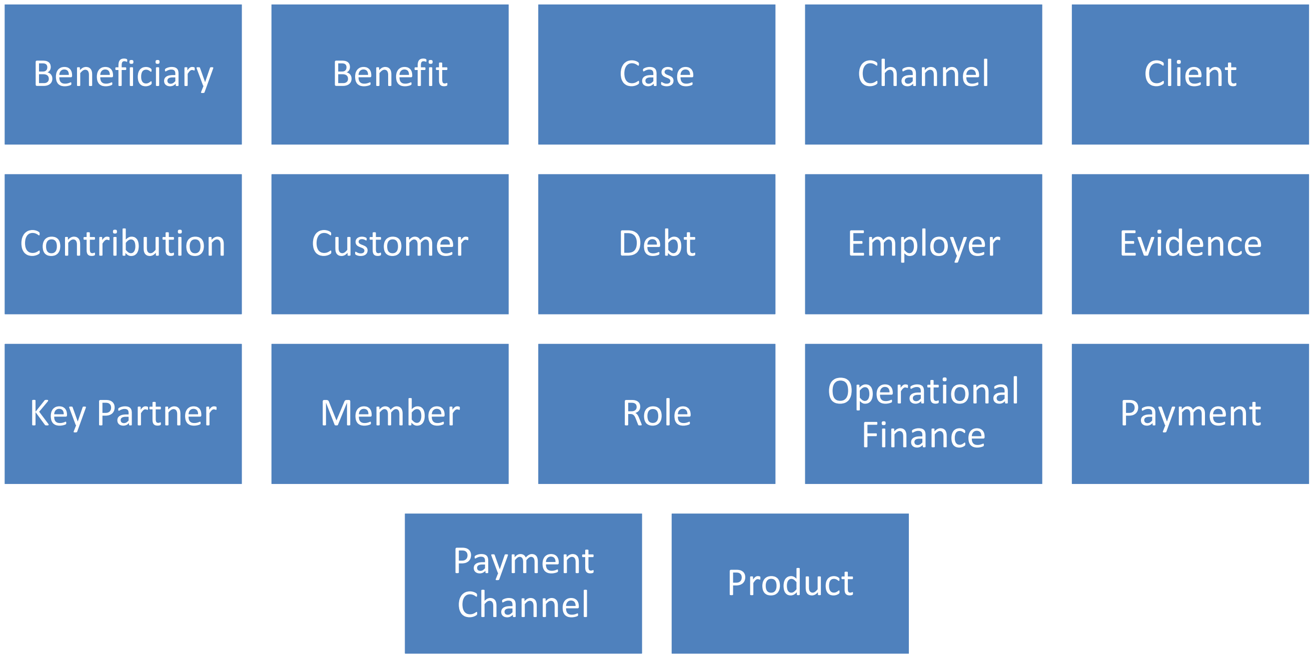


Figure 15 Key data entities

Below are the descriptions of the key data entities.

Information	Definition
Beneficiary	A person who has received or is still receiving the benefits after application of the product rules
Benefit	The actual monetary value that a beneficiary is entitled to as a result of applied product rules
Case	A formal request triggered by a client executed by a predefined set of actions sequenced and tracked with the purpose of fulfilling a formal request within a predetermined time frame
Channel	A communication route for communication from and to our clients, members and beneficiaries
Client	Any entity who interacts with the Administrator in his own capacity or on behalf of another person
Contribution	A payment for the purpose of building a fund for a specific purpose

Customer	An organisation on whose behalf the Administrator (GPAA) administers its benefits
Debt	A sum of money that is owed because of the various debt payment arrangements between a member, employer and the GPAA
Employer	An organisation that employs the member and usually is responsible for paying the contribution
Evidence	Tagged images or structured data representations submitted to the Administrator as proof to validate information
Key Partner	Organisations that the Administrator is dependent on so that services are delivered effectively and efficiently
Member	A person who has been admitted to a fund and is entitled to benefits as described in the product rules
Role	An organized group of people within GPAA with a particular purpose
Operational Finance	The management of money flowing into and out of bank accounts
Payment	The actual benefit of a recipient that is paid into a specific bank account
Payment Channel	A payment route to enable payment to our beneficiaries
Product	A set of rules that define the eligibility (conditions of receipt) of an individual and potential benefit(s) (calculation formula) that a product must provide to this individual in the occurrence of life events as described in said rules

Additional Data Entities:

Additional data entities can include those listed below.

1. **Client Information**: Details about the individual or employee participating in the pension fund.
    - Name
    - Date of Birth

- Social Security Number or equivalent unique ID
- Contact Information
- Employment Details
- Beneficiaries

2. **Employer Information**: Details about employers who have pension plans for their employees.
    - Employer Name
    - Employer Address
    - Contact Information
    - Number of Employees
    - Pension Plan Details
3. **Pension Plan Details**:
    - Plan Type (Defined Benefit, Defined Contribution, etc.)
    - Contribution Rates
    - Vesting Period
    - Withdrawal Rules
4. **Financial Transactions**:
    - Contributions (by participants or employers)
    - Distributions (pensions paid out)
    - Investment Returns
    - Fees and Charges
5. **Investment Details**:
    - Asset Types (stocks, bonds, real estate, etc.)
    - Portfolio Composition
    - Investment Performance
    - Risk Metrics
6. **Benefit Claims**:
    - Claim Type (retirement, disability, etc.)

    - Claim Status
    - Payout Amounts

7. **Regulatory and Compliance**:
    - Audit Records
    - Regulatory Reports
    - Compliance Violations

8. **User Access and Security**:
    - User Roles
    - Access Logs
    - Security Breaches

4.1.2 Data Sets Classification

GPAA's data footprint would have a wide range of data entities to manage its operations.

The data can be classified into the data sets below, for data management purposes.

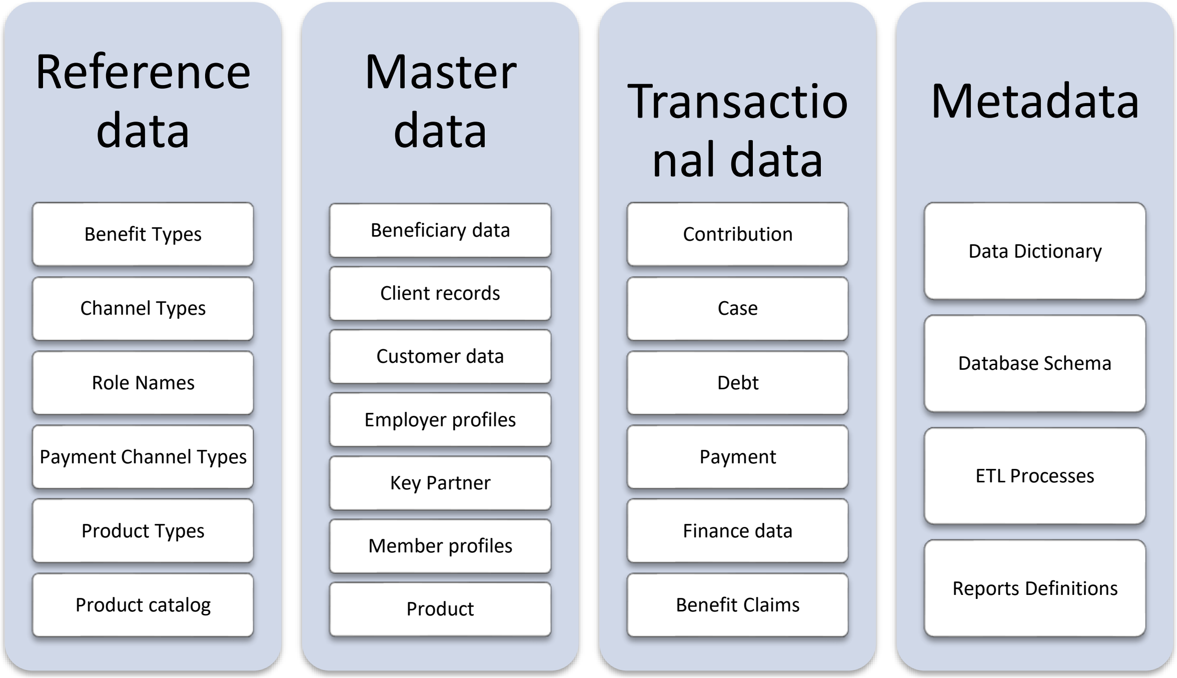


Figure 16 Data Sets Classification

- **Reference Data**: This is a set of values or classification schemas referred to by systems, applications, data stores, processes, and reports. In the context of pension funds and benefits administration, reference data refers to the set values or classification schemas used to categorize and validate information such as benefit plan types, contribution rates, or regulatory codes.
  It serves as an authoritative source of information to maintain consistency across the organization.
- **Master Data**: This represents the business objects that contain the most valuable, agreed upon information shared across an organization. It plays a distinct role in a company by providing a common point of reference across different disciplines and techniques used to process, store, and organize data.
  For pension funds, master data includes the core details about members, beneficiaries, and employers, such as personal information, contribution history, and benefit entitlements. This data is crucial for managing member accounts, calculating benefits, and ensuring accurate and timely payments.
- **Transactional Data**: This type of data is generated during transactions and typically consists of time, numerical value, and reference to master or reference data. Transactional data in pension funds consists of records of individual transactions, such as contributions, withdrawals, benefit disbursements, and investment activities. It helps in tracking the day-to-day operations, monitoring fund performance, and member account management.
- **Metadata**: Metadata is data about data, providing a description or context of the actual data, making it easier to retrieve, use, and manage. It is essential in data management as it helps in organizing and processing the data effectively.
  In benefits administration, metadata is vital for describing, managing, and documenting the pension data, such as data origin, format, usage, and update history. It assists in ensuring data quality, compliance, and efficient data management processes.

The data needs to be managed consistently across the different applications and data stores.

The relevant components need to be identified as the relevant sources for each of the data entities stated.

4.1.3 The Data Models

GPAA's data models determine which data entities are required by GPAA, what entities must be carried for each entity and what are the relationships between the various entities.

The data models take the entities described in the information model described in the business architecture and turn them into practical, concrete and manageable entities.

The models shall need to be defined at the following levels:

- Conceptual Data Model – the conceptual data model is a structured business view of the data required to support business processes and record business events.
- Logical Data Model – describes the data in details including all the entities, all the attributes of each entity and all the relationships between the entities.
- Physical Data Model – represents how the data is created in the database.

GPAA is currently carrying out an initiative to define a conceptual data model across all systems at the GPAA. The data models detail for some of the components are available in various artefacts and shall need to be modelled in a suitable modelling tool. For these reasons this document shall not define the detail of the data models.

The Enterprise Data Models for the organization need to be modelled to represent the business and technical aspects of the enterprise architecture and operations.

The conceptual data model below represents the high-level data entities identified and shall need to be included in the enterprise data models for the relevant components.

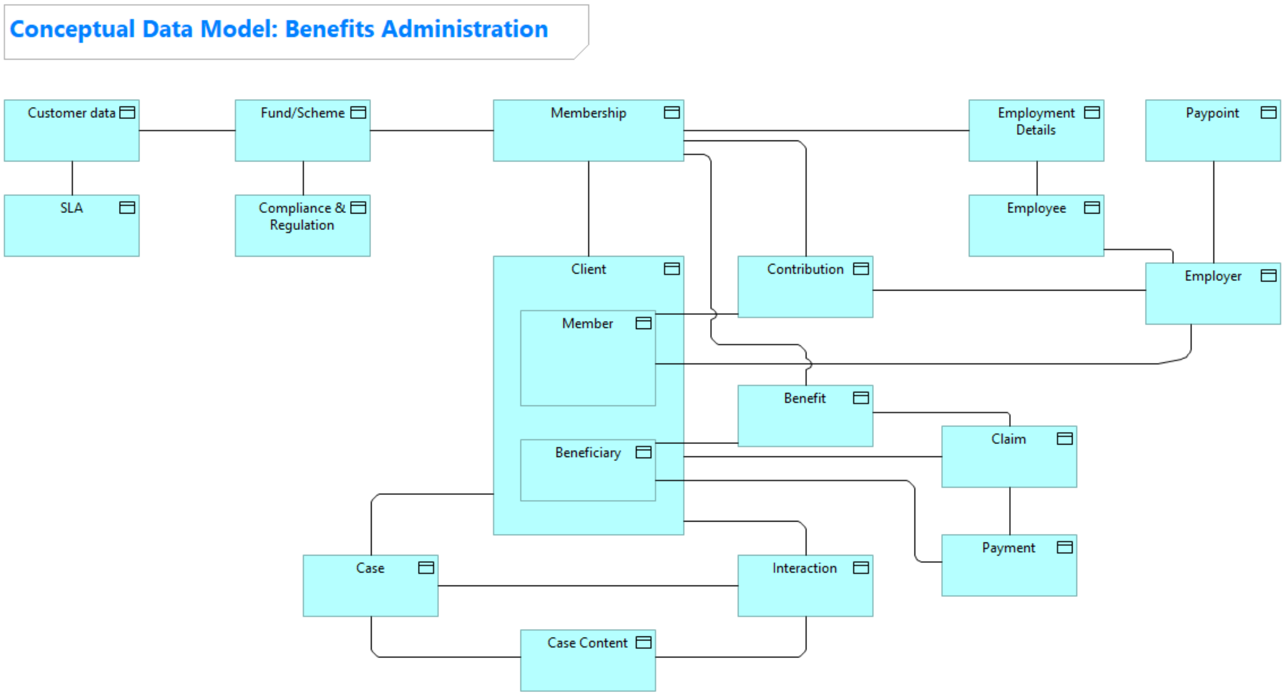


Figure 17 High Level Conceptual Data Model for Core Operations

GPAA Logical Data Model: A logical data model has been defined but requires updates.

The logical data model for the GPAA data in the CDR has been documented in the other GPAA ICT CDR and Data Architecture artefacts. Below is a snapshot.

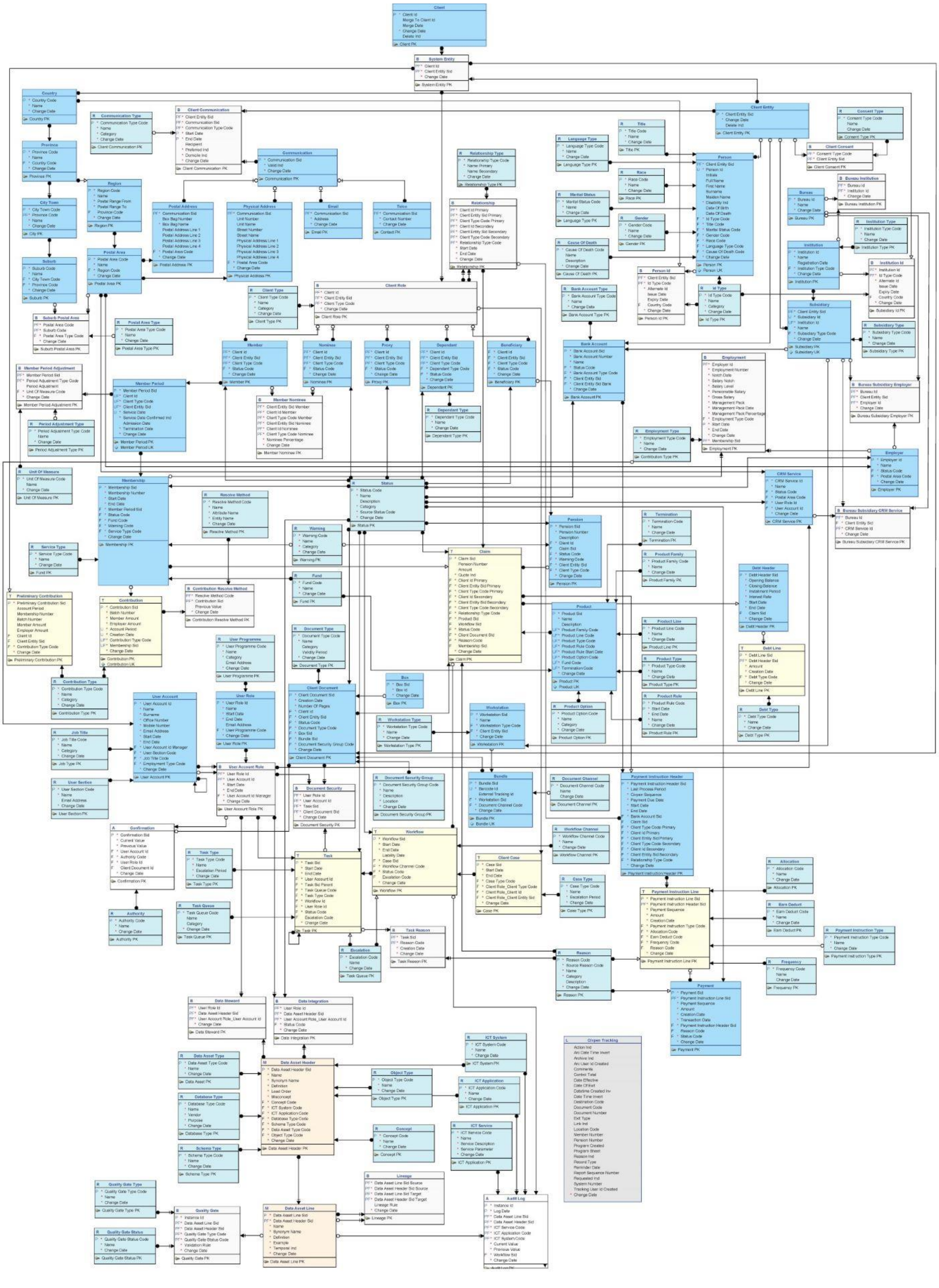


Figure 18 CDR Logical Data Model

4.1.4 Data Stores

Data stores refers to the type of stores and to the store management systems used at the GPAA.

The following types of data stores are used at the GPAA:

Platform Type	Technology Platform	Usage
Database Management Systems	Oracle Databases	Used as the database to all member/pensioner related structured information.
	SoftwareAG Adabas	Used by CIVPEN for storing member/pensioner related information
	Microsoft SQL Server	Used for non-core functions at the GPAA such as SharePoint, the Intranet and various other document stores for various initiatives at GPAA.
Content Management System	Oracle WebCenter Content	Used for storing contents of documents such as PDF documents, TIFF documents and others.
File systems	Various	Used to store various file types such as Word documents, excel document and PowerPoint documents.
Business Intelligence Platforms	Business Intelligence Architecture Framework	Data consolidation and preparation for reporting, analysis and distribution.

Business Intelligence Architecture Framework

GPAA has defined a Business Intelligence Framework and adopted a Bimodal approach for implementation of the architecture.

There are two architectural areas in the Conceptual view below, the Foundation areas of BI (Grey blocks) and Mode 2 of the Bimodal (Red blocks). Both areas form an integrated view of the Conceptual Model:

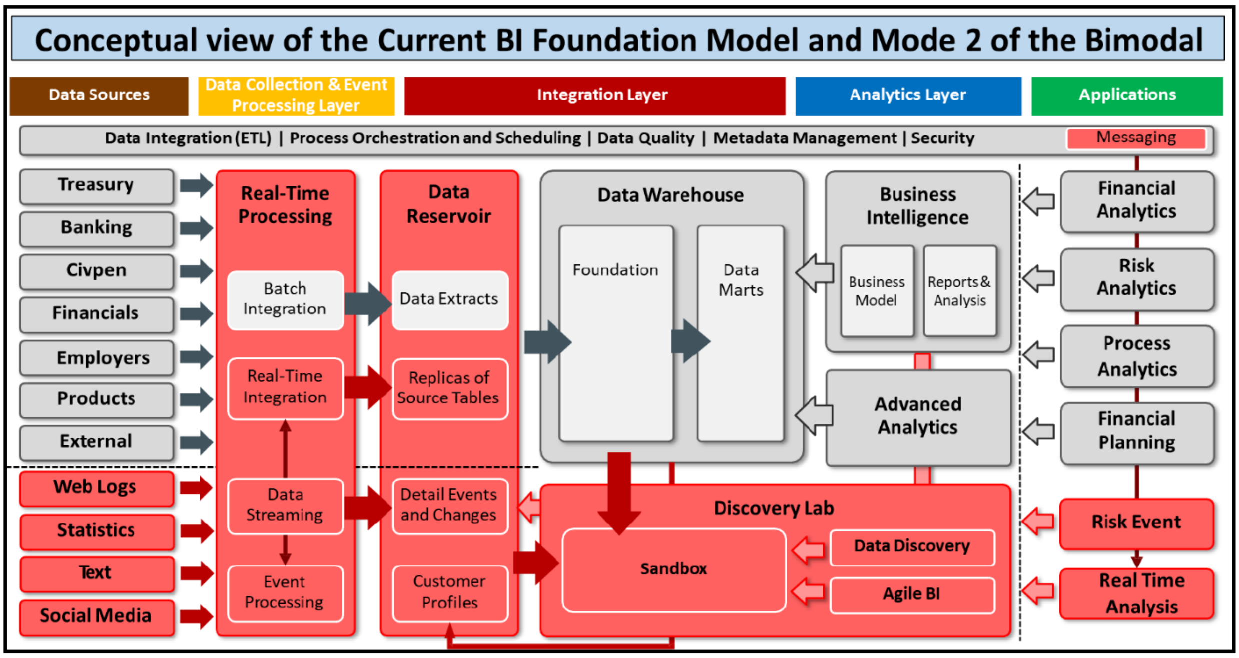


Figure 19 Conceptual view of the Foundation Model and Mode 2 of the Bimodal

Below is a technology view of the Current BI Foundation Model and Mode 2 of the model.

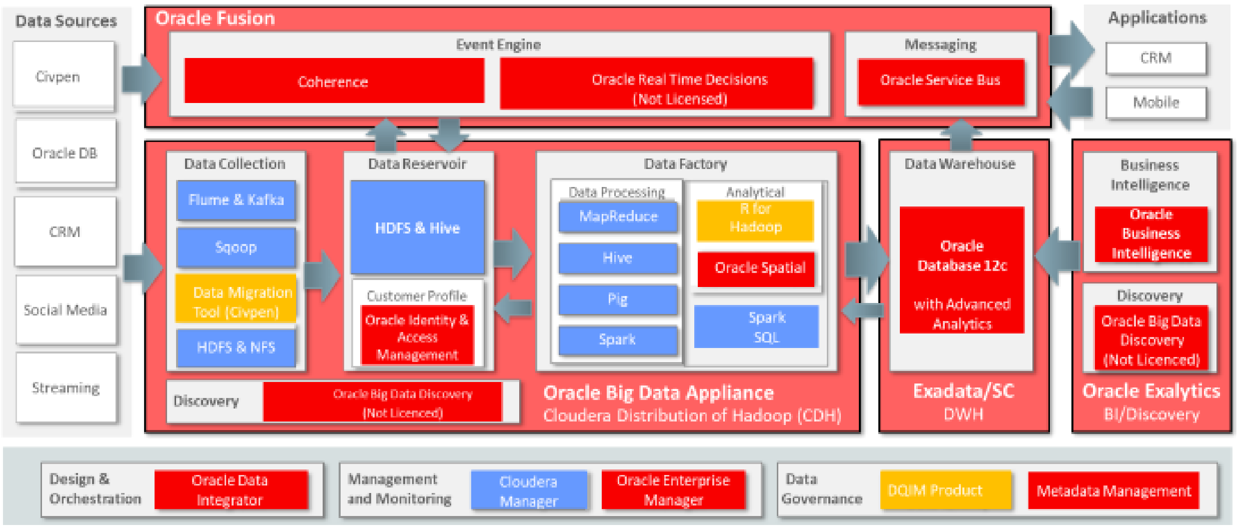


Figure 20 Technology view of the Foundation Model and Mode 2 of the Bimodal

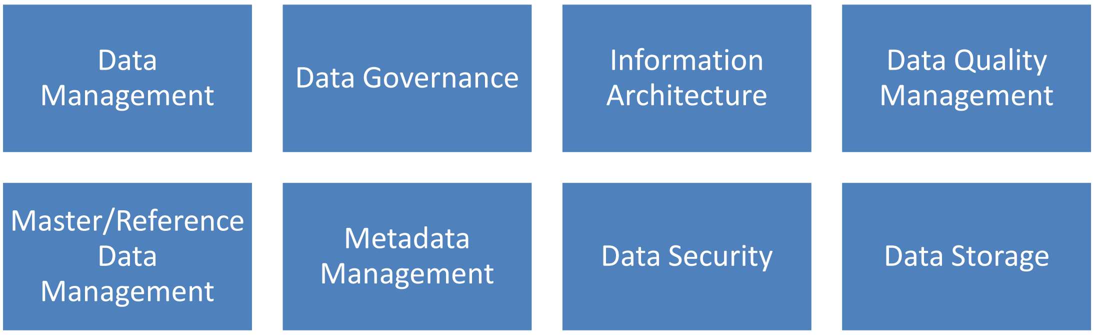
GPAA adopted Oracle as implementation partner for the execution of the Technical Architecture Design and Implementation phase.

- The red blocks: represent Oracle products. This includes all the Foundation model components.
- Yellow blocks: other vendors
- The blue blocks are mainly big data products

4.1.5 Enterprise Data Management

The Modernisation Programme architecture shall be aligned to the strategic Enterprise Information Management Strategy, Architecture and Standards.

The following illustrates some of the enterprise data management and governance capabilities and aspects that need to be taken into consideration for this initiative as it incorporates data that is/shall be moved, managed, and shared across systems, across the organization and externally.



Data Management	Data Governance	Information Architecture	Data Quality Management
Master/Reference Data Management	Metadata Management	Data Security	Data Storage

These aspects have already covered in the GPAA Enterprise Data Architecture Framework

Data Management

Implement a centralized data management system that ensures data is stored in a structured, organized manner. Use cloud-based solutions with redundancy to prevent data loss and enable real-time updates. Implement version control systems to track historical data changes.

Data Governance

Ensure that the Data Governance Council comprises of representatives from key departments. This council will be responsible for setting data-related policies, handling disputes, and ensuring data integrity. Regular reviews and updates of policies should be scheduled.

Consider implementation of data governance tools.

Information Architecture

Design a clear, logical data model that captures the relationships between different data entities. Implement a robust Enterprise Resource Planning (ERP) system tailored for pension administration, ensuring all data is interconnected.

Data Quality Management

Implement data quality management and data validation tools that automatically check data for inconsistencies or anomalies upon entry. Schedule regular data audits, where a team reviews a random subset of the data for accuracy and consistency.

Implement data quality management across the landscape.

Master and Reference Data Management

Set up a Master Data Management (MDM) platform to maintain a 'single source of truth.' This platform will ensure that master data is consistently used across all systems. For reference data, implement a regular review process to keep it current and relevant.

Metadata Management

Implement metadata management tools that can automatically document, store, and track changes to metadata. Create a metadata repository that is accessible to all relevant stakeholders, ensuring they understand the context of the data they work with.

Data Security

Adopt advanced encryption techniques to secure data both in transit and at rest. Utilize multi-factor authentication for access to sensitive data. Regularly back up data in encrypted, geographically distributed locations. Implement intrusion detection systems and regularly update security protocols to stay ahead of potential threats.

The data management implementation strategy must align with the GPAA Enterprise-wide data strategy and frameworks.

5 Applications Architecture

The applications architecture describes the software applications within the organization and how the applications interact with each other to meet organizational requirements.

5.1 Layered Architecture Context

The layered Conceptual Architecture context below aims to describe the Enterprise Architecture (EA) view that provides a holistic and structured approach to understanding and designing an enterprise. This view aids in making strategic decisions, aligning IT and business, and ensuring a consistent, efficient operation of the organization.

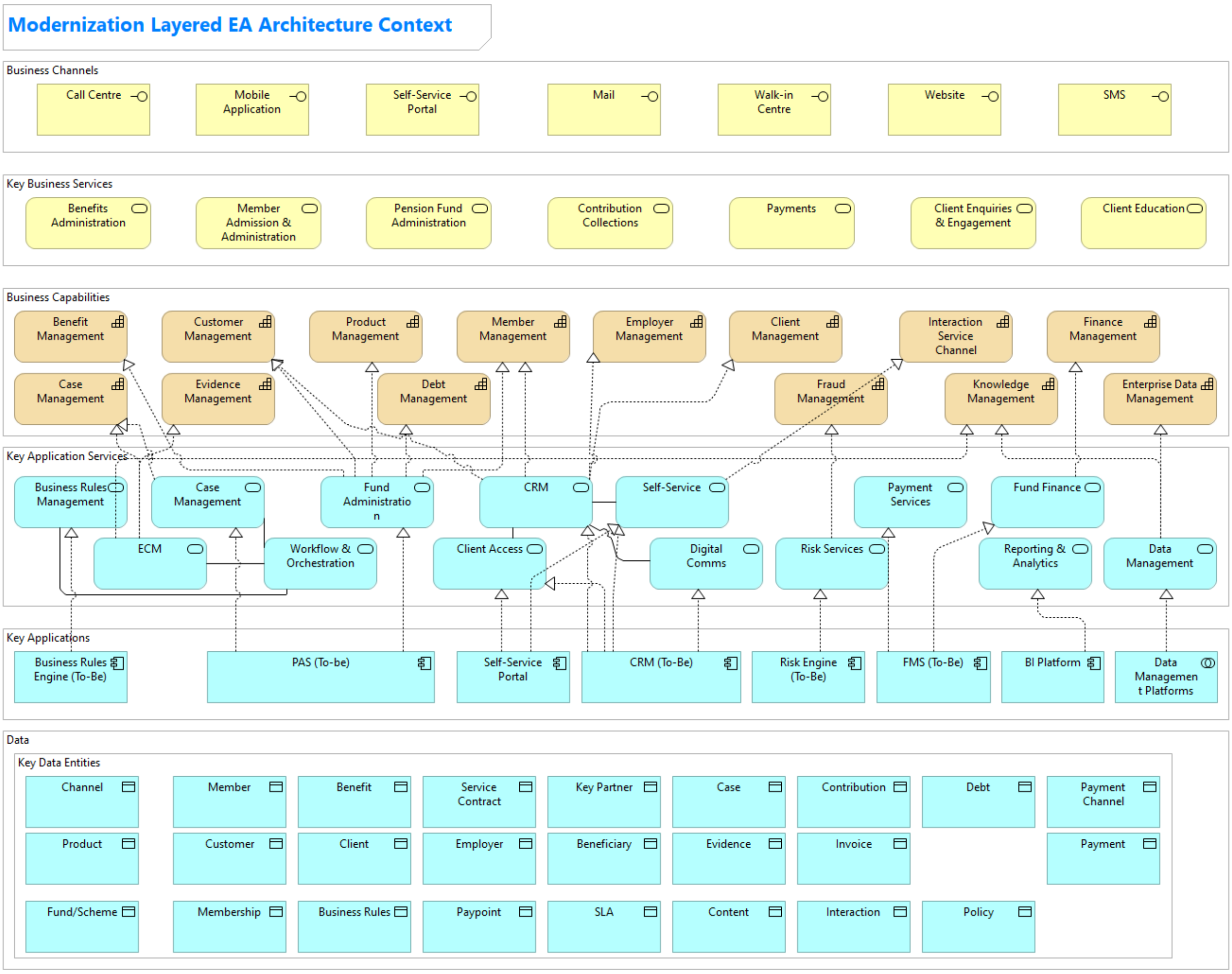


Figure 21 Layered Conceptual Architecture context.

Business Channels:

- **Description**: These are the touchpoints or mediums through which GPAA business interacts with its customers, stakeholders, or other entities. Channels can be physical (like a desk or office) or digital (like a website or mobile app).
- **Significance**: Understanding business channels is crucial because they directly influence the customer experience, and they can determine how products or services are delivered to the market.

Business Services:

- **Description**: Business Services represent the offerings that the enterprise provides to its customers, either internally or externally. They are high-level descriptions of the value provided. The services depicted above are provided to external parties.
- **Significance**: By defining business services, Organisations can clearly communicate what they offer and can structure their internal processes around delivering these services efficiently.
- **Examples**: Fund Administration, Member Administration

Business Capabilities:

- **Description**: Capabilities define what a business can do or its abilities in operational terms. They are the foundational building blocks that enable the execution and delivery of business services.
- **Significance**: Business capabilities provide a stable view of the business, unaffected by organizational changes or technological choices. They help in identifying gaps, redundancies, or areas of strength.
- **Examples**: These are the defined GPAA business capabilities from the Capability Model.

Key Application Services:

- **Description**: These are the technical services that underpin and support the business services and capabilities. They often map to specific IT functions or processes.
- **Significance**: Application services are crucial for the IT and business alignment. They ensure that the IT systems provide the right functionalities to support and empower the business functions.
- **Example**: A Payment Processing service, a CRM service, or a Client Access service are examples of key application services.

Key Applications:

- **Description**: These are the actual software applications or systems that implement the application services. This layer focuses on specific IT solutions, products, or platforms.
- **Significance**: Understanding key applications helps in assessing technology investments, managing vendor relationships, and ensuring that the IT landscape is not overly complex or redundant.
- **Example**: The envisaged PAS, CRM and FMS systems, or a BI solution can be considered as key applications.

The viewpoint above is just a high-level view indicating the key elements of each layer. In the EA Model and Repository, the model has the detailed relationships and can generate various viewpoints that depict the component and layer relationships to support any questions.

In the context of Enterprise Architecture, this layered view ensures that:

- There's a clear alignment between business needs and IT solutions.
- Decisions made at any layer are consistent with and supportive of the layers above and below it.

By having a clear view of each layer and the relationships between them, Organisations can make informed decisions, reduce risks, optimize processes, and drive innovation.

5.2 Application Services

GPAA has a wide range of technology and application capabilities provided by the technology landscape. Application Services aim to group and categorize the capabilities that the technologies provide to the other layers of the enterprise.

An application service is realized by one or more application functions that are performed by the component. It may require, use, and produce data objects. It represents an explicitly defined exposed application behaviour.

The following Application Services in the table below have been defined for the GPAA, primarily focussing on those required for Modernization.

These application services realize the business services and overall operating model. These Application Services are in turn realized by the supporting technology components and applications.

These have been modelled and mapped in the Archi GPAA EA Model and repository.

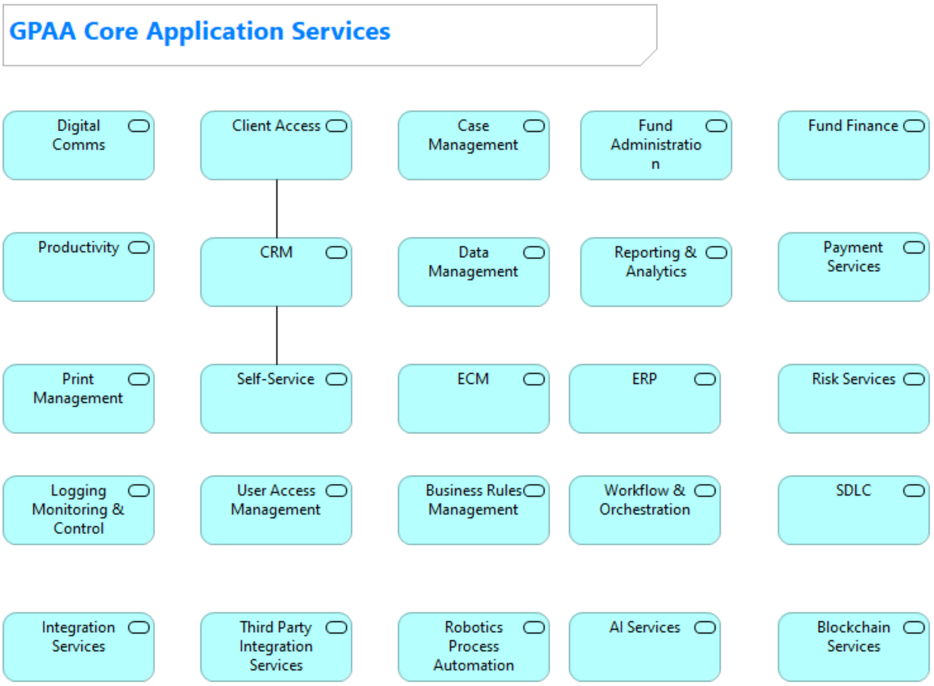


Figure 22 Application Services

Below are basic descriptions for each service.

- **Business Rules Management**
  The process of defining, deploying, monitoring, and maintaining the decision logic that drives operations in the agency. It helps to automate decisions, ensuring consistency and compliance with pension policies.
- **Case Management**
  Managing the life-cycle of specific cases (e.g., pension applications, claims, or grievances) by organizing, prioritizing, and coordinating resources and tasks.
- **Client Access**
  The methods and channels through which clients (e.g., pensioners, employees) can access services, information, and support.
- **CRM (Customer Relationship Management)**
  Systems and strategies for managing the agency's relationships and interactions with current and potential customers, pensioners and other stakeholders.
- **Data Management**
  Enterprise Data Management (EDM) refers to the ability of an organization to precisely define, easily integrate, and effectively retrieve data for both internal applications and external

communication. For GPAA, these capabilities are vital to ensure accuracy, compliance, regulatory adherence, and effective service delivery.

Below are key capabilities that fall under EDM. They have been modelled as technology functions in the model and repository.

- **Data Governance**:
    - Establishing policies, procedures, and standards to ensure data is consistent and used appropriately. It involves defining roles and responsibilities related to data management and ensuring compliance with internal and external regulations.
- **Data Quality Management**:
    - Ensuring the accuracy, completeness, consistency, reliability, and timeliness of data. It includes validating, cleansing, and enriching data to maintain its quality throughout its lifecycle.
- **Master Data Management**:
    - Managing the organization's critical data (like beneficiaries, employees, and service providers) by integrating data across the enterprise to create a single, accurate view of business-critical information.
- **Metadata Management**:
    - Managing and documenting the information about the data such as its structure, location, and usage. It enables better understanding and usage of data assets.
- **Data Integration**:
    - Combining data from different sources to provide a unified view or dataset. It involves ETL (extract, transform, load) processes, data consolidation, and data propagation.
- **Data Security and Privacy**:
    - Protecting data from unauthorized access and ensuring that privacy is maintained. It includes encryption, access control, data masking, and audit logging.
- **Data Archiving and Retention**:

    - Storing, archiving, and ensuring data is retained for as long as necessary to meet legal, regulatory, and operational requirements.

- **Data Lifecycle Management**:
    - Managing the flow of data through its lifecycle from creation and initial storage to the time when it becomes obsolete and is deleted.
- **Data Warehousing and Data Lakes**:
    - Storing large volumes of structured and unstructured data and enabling complex queries and analysis. It supports business intelligence, reporting, and analytics.
- **Business Intelligence and Analytics**:
    - Turning data into actionable insights through reporting, dashboards, data visualization, and advanced analytics.
- **Data Cataloguing**:
    - Creating an inventory of data assets through the discovery, description, and organization of datasets, making it easier for users to find, access, and manage data.
- **Data Modelling and Design**:
    - Defining the structure, organization, and relationships between different data entities to support data storage, integration, and retrieval.

- **Digital Comms (Communications)**
  Utilizing digital channels such as email, web chat, and social media to communicate with internal and external stakeholders.
- **ECM (Enterprise Content Management)**
  Systems for capturing, managing, storing, preserving, and delivering content related to organizational processes.
- **ERP (Enterprise Resource Planning)**
  Integrated management of core business processes, often in real-time and mediated by software and technology.

- **Fund Administration**
  Managing and overseeing the operations and regulatory compliance of the pension fund, including accounting, reporting, and auditing.
- **Fund Finance**
  Managing the financial aspects of the pension fund, including investments, allocations, disbursements, and forecasting.
- **Human Capital Management Services**
  Managing the agency's workforce, including hiring, training, payroll, benefits, and performance management.
- **Integration Services**
  Connecting different IT systems, applications, and data, both within the organization and with external partners.
- **Logging, Monitoring & Control**
  Tracking, reviewing, and managing the events, transactions, and operations within the IT systems to ensure security, performance, and compliance.
- **Payment Services**
  Managing and executing payment transactions, such as disbursing pensions to beneficiaries.
- **Print Management**
  Overseeing the production, allocation, and use of printed materials within the agency.
- **Productivity**
- Tools and processes that enhance the efficiency and effectiveness of the agency's operations and workforce.
- **Reporting & Analytics**
  Generating reports and using analytical tools to gain insights, support decision-making, and measure performance.
- **Risk & Audit Services**
  Enterprise Risk and Audit technology services refer to the set of tools, systems, and processes that an organization uses to identify, assess, manage, and monitor risks, while also ensuring compliance with laws, regulations, and internal policies. These capabilities help in conducting audits efficiently, ensuring that the organization is operating effectively and that risks are mitigated appropriately.
- **SDLC (Software Development Life Cycle)**
  The process of planning, creating, testing, deploying, and maintaining software applications or systems.
- **Self-Service**

Enabling clients, customers and employees to perform tasks and access information on their own, typically through online portals or automated systems.

- **User Access Management**

  Defining and managing the access rights of individuals to the IT systems and data.
- **Utilities/Facilities Management**

  Managing the physical and utility resources such as buildings, equipment, and energy.
- **Workflow & Orchestration**

  Designing, optimizing, and automating the flow of tasks and activities within the organization.

5.3 Application Landscape

The Application Landscape refers to the portfolio of software applications and computational entities within the organization. It provides a clear picture of the software ecosystem of an organization, aiding in making informed decisions about IT investments, mitigations, and future planning within the context of Enterprise Architecture.

This is crucial as it enables the integration and alignment of business processes and IT infrastructure within the organization, which is a fundamental aspect of EA.

This section depicts the current and future application landscape with respect to the services and capabilities in the scope of the Modernisation Programme.

5.4 As-Is Application Landscape

The current landscape is shown below. The applications have been grouped by the services and capabilities that they provide. The applications in grey shall be decommissioned and replaced by the solutions that the programme aims to deliver.

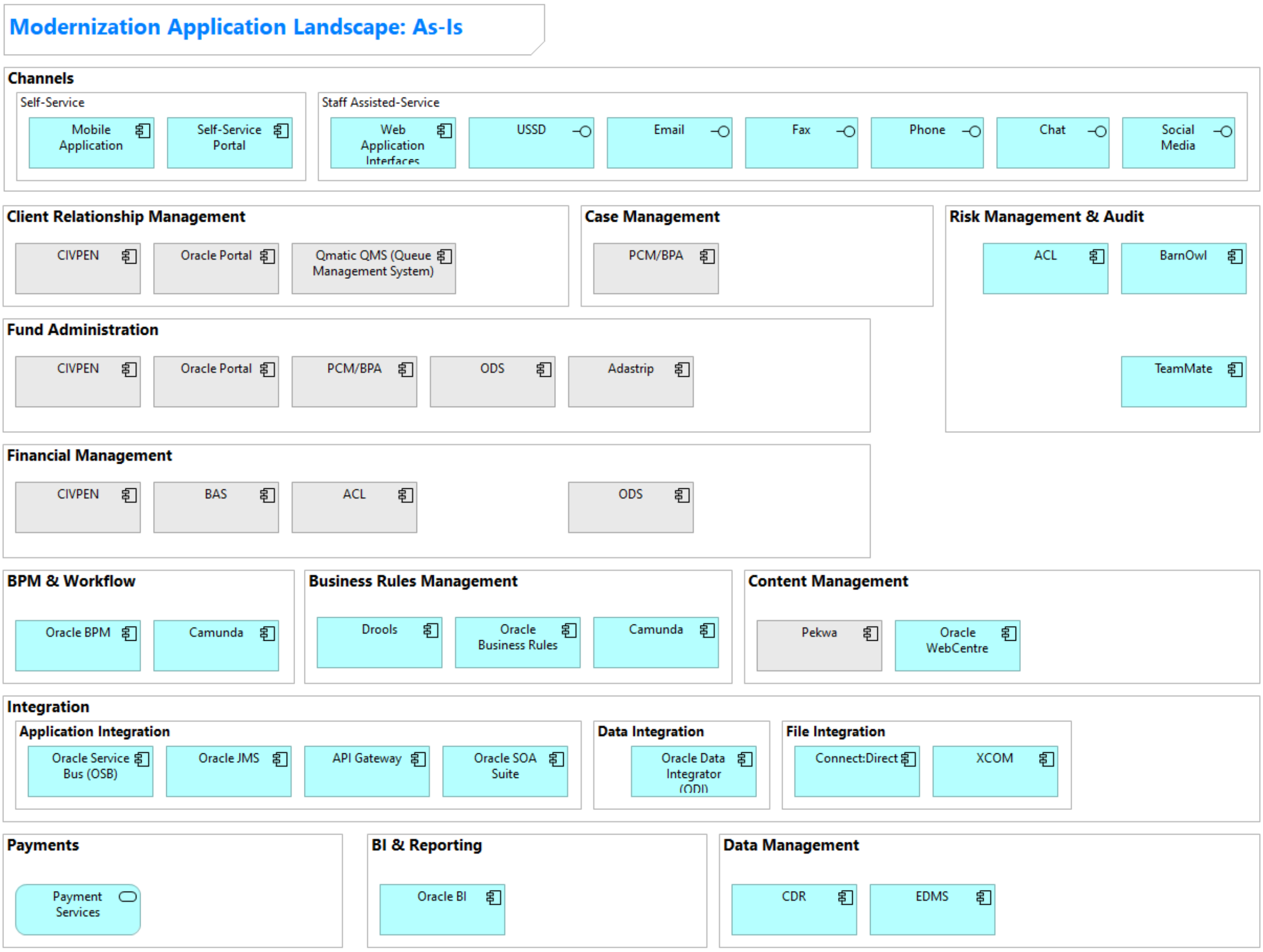


Figure 23 As-Is Application Landscape

The GPAA currently has several applications collaborating in fulfilling the key Modernisation requirements, i.e., CRM, Pension Administration and Financial Management.

Application Catalogue

Below are the key applications that support the GPAA business.

Productivity

There are various productivity applications including the following:

- Microsoft Office 365 E5 licensed products: These include MS Word, MS Excel, MS PowerPoint, MS Outlook, MS Visio and MS Project
- SharePoint
- Project Server is being implemented.

Risk & Audit

The following solutions are currently implemented.

- ACL
- TeamMate
- BarnOwl

Digital Communication

Digital Communication is used platform for sending emails and SMS to pre-defined recipients, mostly members and pensioners.

Integration to other communication media such as WhatsApp and USSD is supported.

Frequently used by the GEPF to communicate with members and pensioners.

CRM

Current tools used by Call Centre and Walk-in Centre agents are CIVPEN and Oracle Portal's General Enquiries. Both are mature, stable products but with some drawbacks.

CIVPEN – only provides a green screen user interface which presents some challenges.

Oracle Portal General enquiries – runs on a platform for which support is provided on a “best effort” basis.

This capability is to dovetail with the Customer Experience/Voice of the client project.

Computer Telephony Integration (CTI) service is provided by In2IT. Includes telephony integration, call centre application, workforce management and various dashboards and management reports. The requirements and the integration with back-end systems to be reviewed.

Queue Management System (QMS) is used for managing the physical queues in the walk-in centres and regions and it currently works well.

Client Accessibility

- GEPF Mobile App – in final stages of development
- Self Service Portal – in integration with back-end services (including integration to identity management services).

This area requires implementation of awareness campaigns.

Enterprise Resource Planning (ERP)

- HR – PERSAL
- Finance – AccPac and CIVPEN
- SCM – Manual

The ERP area requires overhauling.

Use of IFMS is considered for some of the following projects:

- Leave Management
- Performance Management
- Contract Management
- SCM
- Finance

In discussions with National Treasury to use their IFMS licenses.

Fund Administration

Several applications collaborate for this service, including the following;

- CIVPEN – General fund administration activities
- PCM/BPA – exit Claim Processing
- Oracle Portal – Funeral Benefits workflow, Benefit calculator, General Enquiries
- ODS – Tax Directive Interface
- BankServ – Interface to BankServ systems to affect benefit pay out to bank accounts.
- SafetyWeb Banking System – interface for benefit payments above R 2 million including to connect with the commercial banks including South African Reserve Bank (SARB) for processing of Telegraphic Transfer (TT) payments, Foreign payments and Bank details verifications.

Application refresh required to replace aging systems: CIVPEN, Oracle Portal, ODS and BankServ Interface.

5.5 To-Be Application Landscape

The target state landscape is shown below. This shows the applications that the programme shall implement and replace the legacy solutions currently in place.

More detail and mapping to the requirements is shown in the ‘Modernisation Requirements Realization’ section of the document.

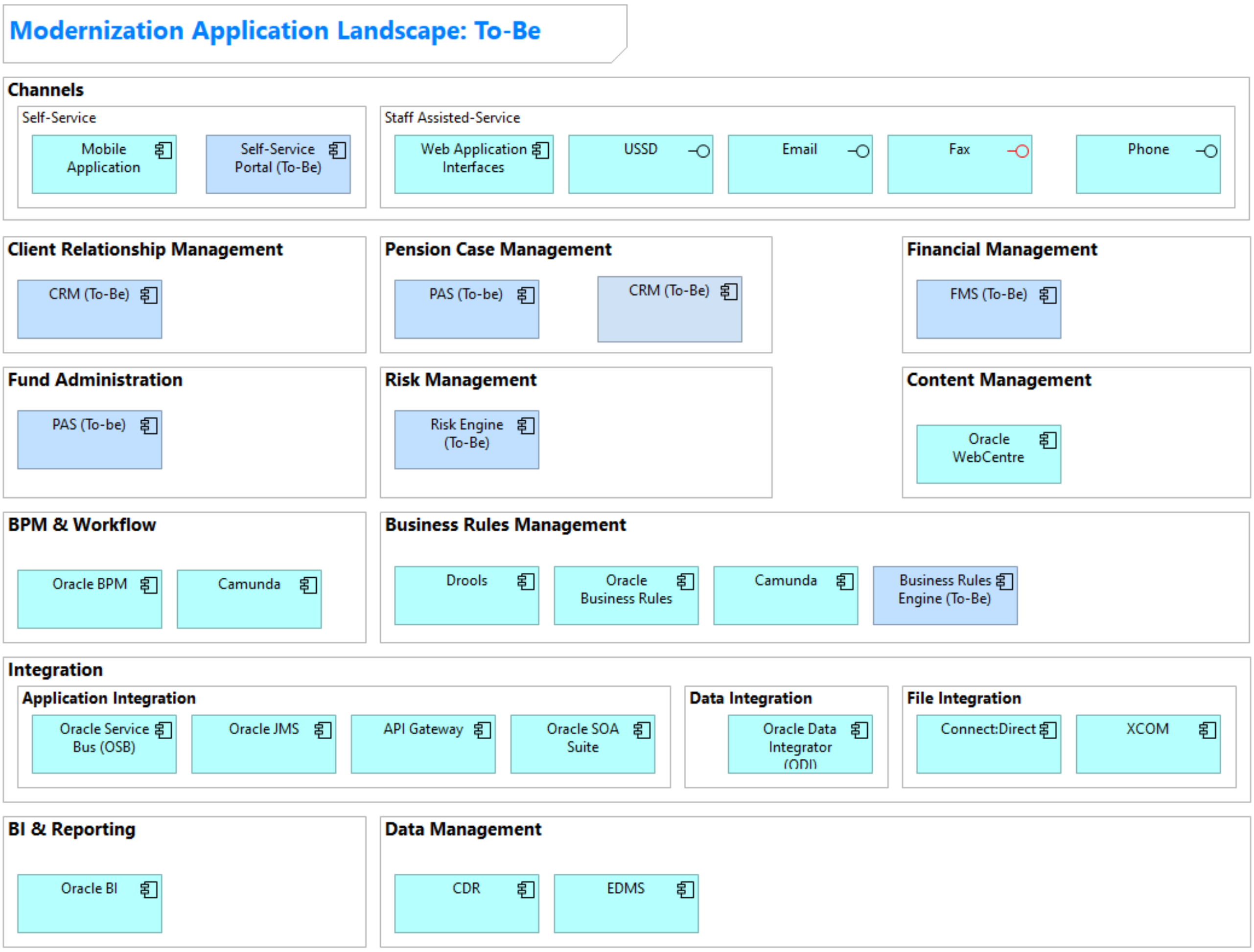


Figure 24 To-Be Application Landscape

The target state landscape aims to replace the legacy applications through a technology refresh for the capabilities in scope, and to create a simplified application landscape with fit for purpose solutions that provide most of the capabilities off the shelf.

5.6 Application Inventory

The Application Inventory is a comprehensive list or catalogue of all software applications that are used within an organization. This inventory serves as a critical resource for managing and optimizing an organization's software assets and supporting various IT and business functions.

Table 9 provides a list of applications in production at the GPAA, their description, pain points and future plans for these applications. These applications are used by GPAA to carry out its mandate.

Table 10 provides a list of applications that are used by GPAA as part of its software development life cycle to develop, install and configure applications for GPAA operational use.

Table 11 provides a list of applications and facilities that are being used to monitor the health of the operational ICT environment of GPAA, identify any emerging issues and enable quick corrective action to prevent deterioration and outage in any of the components of the GPAA operational environment. These applications and facilities are critical in maintaining high availability of the GPAA operational environment.

5.7 Modernisation Requirements Realization

The following section deals with the realization of the defined requirements.

The Modernisation business requirements were defined in the Business Case and Business Requirements documents. This section deals with the realization of those requirements through the envisaged technology solutions.

The views illustrate how the requirements are realized through some Application Services, which are in turn realized through various application solutions.

The associated models have been defined in the Archi repository, GPAA EA Model.

5.7.1 Programme 2.1 Modernisation Requirements Realization

The Modernisation programme must enable or enhance in the operational processes and functions of the National Treasury (NT) funds, or any other fund administered under Programme 2.1.

The GPAA is experiencing high volumes of benefits being processed and finalized after the prescribed time period as required by the Law, policies and/or service level agreements.

The following have been identified causes:

- Delayed submission of the benefit claims.
- Delay time as time spent on the movement of physical documents and/or files between storage and sections or units.
- Delay time as time spent on preparation and allocation of physical documents and/or files for processing.
- Delay time as waiting time for submission of physical supporting documents.
- Delay time as time spent on resolving errors.
- Claims not paid within the prescribed time period.
- Insufficient Change Data rules impacting on data integrity.

This delay also directly or indirectly causes a delay on other dependent processes.

The scope of this documentation is limited to the following capabilities of the Programme 2.1 funds:

Capability	**Description**
Member Information Management	The ability to maintain and manage all membership. information for purposes of administration from the start to the end of the membership.
Contributions Management	The ability to process contributions towards membership.
Benefit Payment	The ability to pay the correct benefit to the correct beneficiary.
Benefit Disbursement Management	The ability to pay correct repeat payments to the correct beneficiary until the end condition occurs.
Service Request Management	The ability to correctly determine the identity of a client and provide credentials to a client for the purpose of using the GPAA systems.
Post Retirement Support Provision	The ability to support pensioners post-retirement with services to reduce the risk of loneliness and social isolation and eventually premature death.
Enterprise Data Management	The ability to plan, execute and oversee policies, practices and projects that acquire, control, protect, deliver, and enhance the value of information and data assets.

The diagram below shows how the associated Modernisation requirements are addressed by the envisaged implementation.

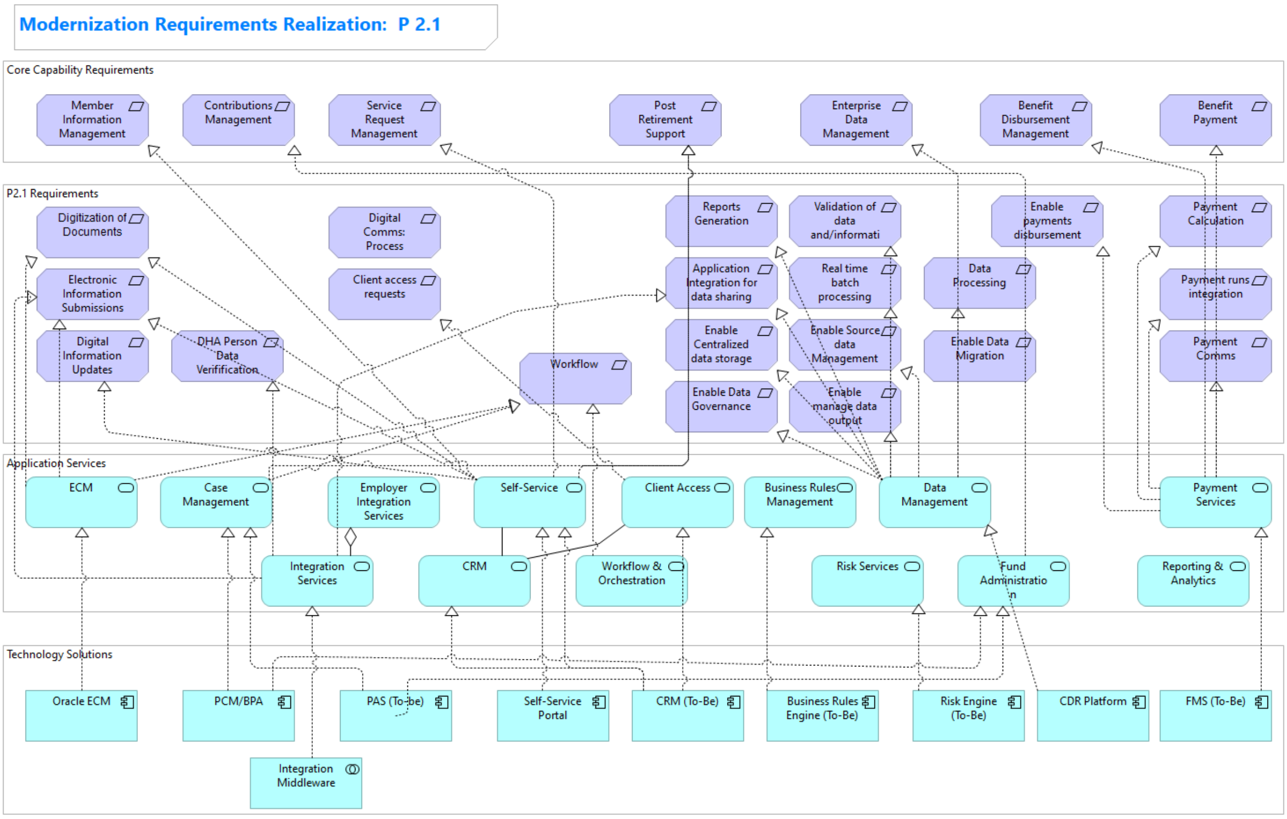


Figure 25 Programme 2.1 Modernisation Requirements Realization

5.7.2 Programme 2.2 Modernisation Requirements Realization

The Modernisation programme must enable or enhance in the operational processes and functions of the Government Employees Pension Fund (GEPF) funds.

The scope of this section is limited to the following capabilities of the GEPF funds:

Capability	**Description**
Member Information Management	The ability to maintain and manage all membership information for purposes of administration from the start to the end of the membership.
Contributions Management	The ability to process contributions towards membership.
Benefit Payment	The ability to pay the correct benefit to the correct beneficiary.

Capability	Description
Benefit Disbursement Management	The ability to pay correct repeat payments to the correct beneficiary until the end condition occurs.
Service Request Management	The ability to correctly determine the identity of a client and provide credentials to a client for the purpose of using the GPAA systems.
Post Retirement Support Provision	The ability to support pensioners post-retirement with services to reduce the risk of loneliness and social isolation and eventually premature death.
Enterprise Data Management	The ability to plan, execute on and oversee policies, practices and projects that acquire, control, protect, deliver, and enhance the value of information and data assets.

The diagram below shows how the associated Modernisation requirements are addressed by the envisaged implementation.

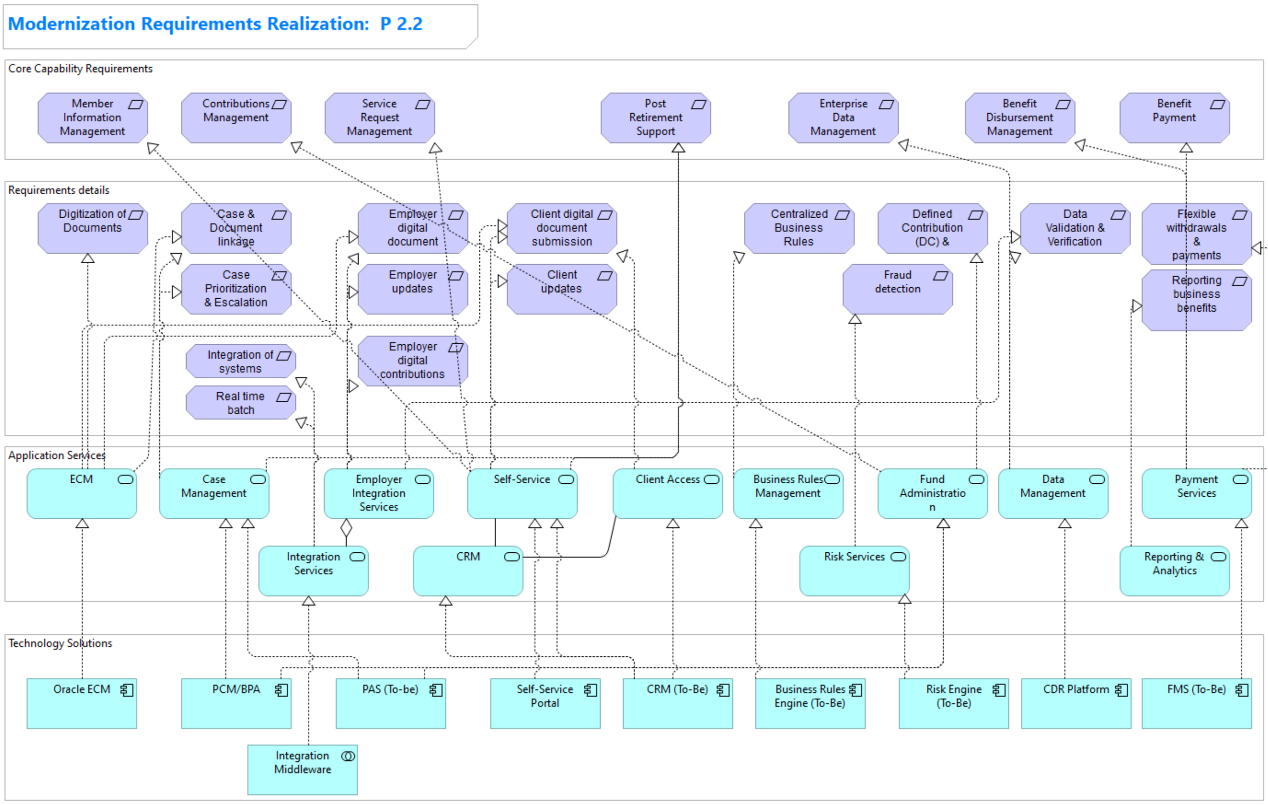

Modernization Requirements Realization: P 2.2
Core Capability Requirements
Member Information Management
Contributions Management
Service Request Management
Post Retirement Support
Enterprise Data Management
Benefit Disbursement Management
Benefit Payment
Requirements details
Digitization of Documents
Case & Document linkage
Case Prioritization & Escalation
Employer digital document
Employer updates
Client digital document submission
Client updates
Centralized Business Rules
Defined Contribution (DC) &
Fraud detection
Data Validation & Verification
Flexible withdrawals & payments
Reporting business benefits
Integration of systems
Real time batch
Employer digital contributions
Application Services
ECM
Case Management
Employer Integration Services
Self-Service
Client Access
Business Rules Management
Fund Administratio n
Data Management
Payment Services
Integration Services
CRM
Risk Services
Reporting & Analytics
Technology Solutions
Oracle ECM
PCM/BPA
PAS (To-be)
Self-Service Portal
CRM (To-Be)
Business Rules Engine (To-Be)
Risk Engine (To-Be)
CDR Platform
FMS (To-Be)
Integration Middleware

Figure 26 Programme 2.2 Modernisation Requirements Realization

5.7.3 CRM Modernisation Requirements Realization

The diagram below shows how the associated CRM Modernisation requirements are addressed by the envisaged implementation.

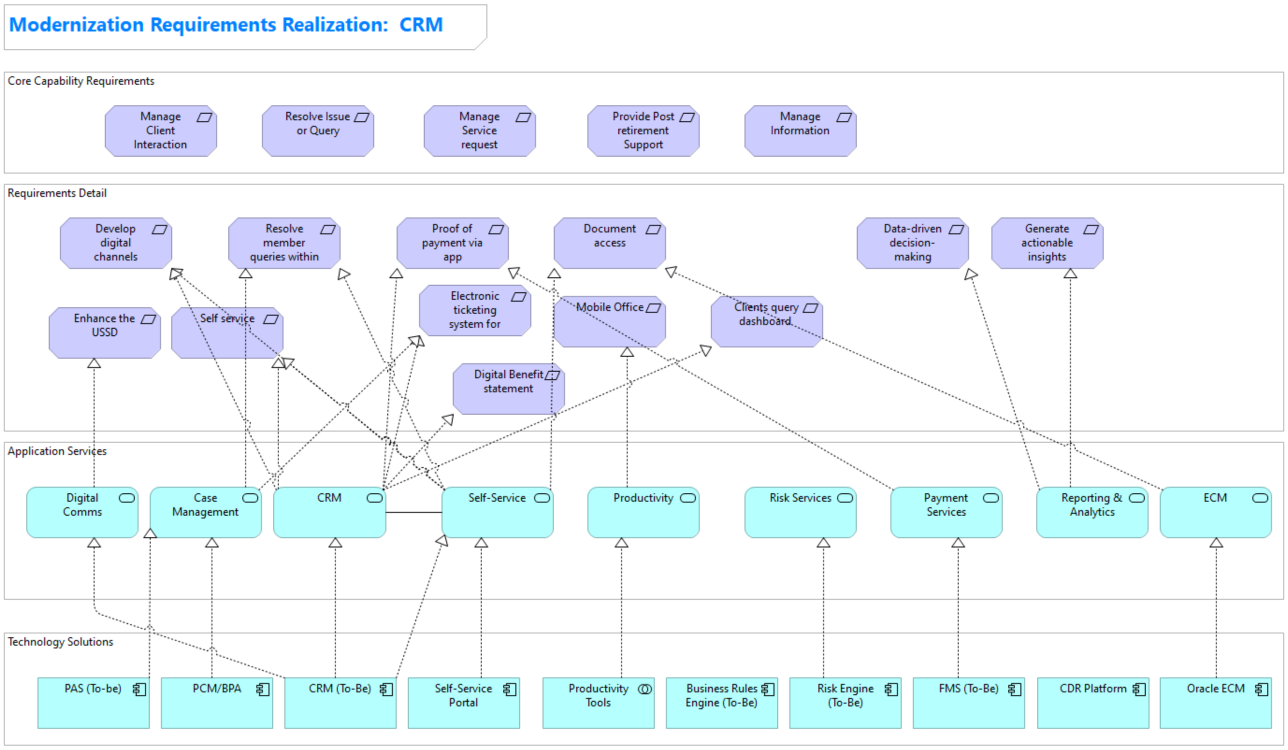


Figure 27 CRM Requirements realization architecture view

5.7.4 FMS Modernisation Requirements Realization

The Financial Services sub-programme manages the bookkeeping, accounting and reporting for the GEPF and NT in line with different rules and regulations.

The GPAA seeks to procure and implement a powerful, well integrated Financial Management System (FMS) to address the current challenges and to add new and enhanced capabilities.

The diagram below shows how the associated FMS Modernisation requirements are addressed by the envisaged implementation.

The following associated Business Capabilities and Value Streams guide the scope of the requirements.

Capability	Value Streams	Description

Financial Management	Funds Management	The ability to manage cash collections and disbursements made by the Administrator and, when appropriate, to transfer cash from those units to parent-level bank accounts managed by the government's treasury unit.
	Cashflow management	The ability to forecast and manage cash inflows, outflows, and cash balances to ensure adequate liquidity.
	Bank Account Information Management	The ability to view the treasury bank accounts by assessing the cash that flows in and out of the bank accounts.
	Treasury Accounting	The ability to ensure that all treasury financial transactions are accounted for and reported on in the administrator’s financial records.
	General ledger Accounting	The ability to collect, account and record all the financial transactions on GPAA’s assets, liabilities, equity, expenses and income on their ledgers according to the accounting model.
	Statutory Reporting	The ability for GPAA to follow processes to submit financial and non-financial information to government agencies according to the laws and regulations applicable to an administrator.
	Finance Reconciliation	The ability for GPAA to compare two different data sets to verify that the information within them is accurate.
	Tax management	The ability for GPAA to comply with tax laws and regulations
	Financial Governance	

The diagram below shows how the associated FMS Modernisation requirements are addressed by the envisaged implementation.

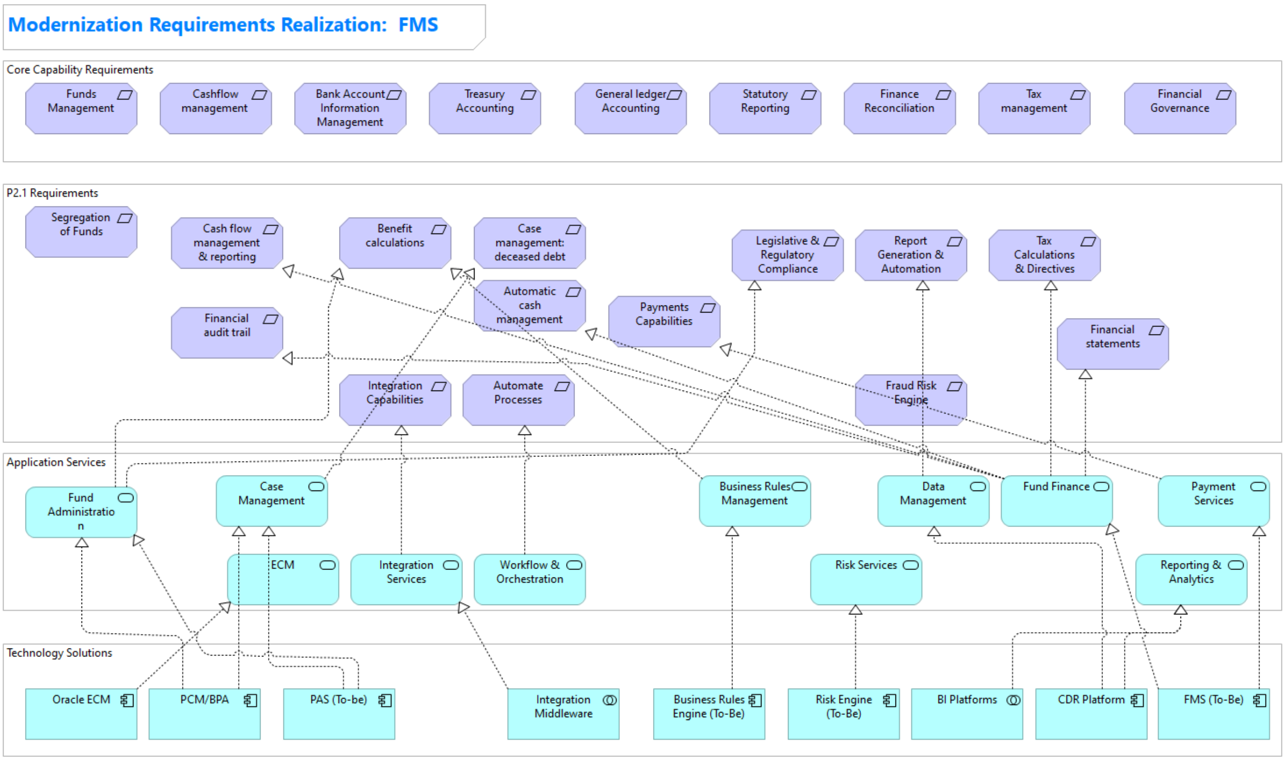


Figure 28 FMS Requirements realization architecture view

5.8 Modern Technology Considerations for Modernisation

The adoption of modern technologies in Pension Fund Administration can significantly improve service delivery, operational efficiency, and financial performance. It is essential to carefully plan the digital transformation journey, considering factors such as current infrastructure, skills availability, and budget constraints. Also, it's important to keep in mind that technology implementation should be accompanied by adequate change management efforts, training, and continuous improvement initiatives to fully reap the benefits.

Some modern technologies hold significant potential for enhancing efficiency, transparency, and service quality in government Pension Fund Administration.

Below are some recommendations for each technology.

<u>Artificial Intelligence (AI) and Machine Learning (ML)</u>

- **AI in Data Analysis**: AI can be employed to analyze large volumes of data to provide insights on pension fund performance, market trends, and potential investment opportunities.

- **AI in Customer Service**: AI chatbots and virtual assistants can provide instant responses to beneficiary queries, guide beneficiaries through processes.
- **AI in Fraud Detection**: Machine learning can also be employed to detect anomalous patterns indicative of fraudulent activities. This enhances the security of pension funds and protects beneficiaries' interests.
- **CRM**: AI can be used to automate customer relationship management (CRM) processes. AI-powered chatbots can handle common queries from pensioners, freeing up time for customer service representatives to focus on more complex cases. Predictive analytics can also be used to anticipate customer needs and personalize service offerings.
- **Pension Fund Administration**: Machine learning algorithms can be used to analyse vast amounts of data. This would help in forecasting pension payouts and ensuring fund sustainability. Additionally, AI can help automate the process of enrolment.
- **Financial Management**: AI can be used for predictive analytics, providing insight for decision-making. Fraud detection systems powered by AI can identify unusual patterns and transactions, helping to prevent fraud and maintain the integrity of the pension fund.

Robotics Process Automation (RPA)

- **Automation of Routine Tasks**: RPA can be used to automate routine, mundane tasks in pension fund administration such as data entry, verification, benefit calculations, and issuing of correspondence. This reduces human error, speeds up processes, and allows staff to focus on more strategic tasks.
- **CRM**: RPA can be used to automate repetitive tasks such as data entry, updating customer records, and handling simple customer queries.
- **Pension Fund Administration**: RPA can be implemented to automate routine tasks such as data verification, updating pensioner records, calculating pension amounts, and disbursing funds.
- **Financial Management**: RPA can automate financial operations including accounts payable/receivable, reconciliation, reporting, and auditing. This would increase efficiency, reduce errors, and allow for real-time financial monitoring.

Blockchain Technology

- **Transparency and Security**: Blockchain can be implemented to maintain a transparent, immutable, and secure record of all pension transactions. It enhances the trust of beneficiaries as they can independently verify transactions and balances.
- **Smart Contracts**: Pension payments can be automated using smart contracts, removing the need for manual processing and reducing errors and delays.
- **Identity Verification**: Blockchain technology can be used to create a secure, decentralized identity verification system. This will ensure that only authorized individuals receive pension benefits, further reducing fraud.
- **CRM**: Blockchain can be used to create a transparent and secure system for handling customer complaints and queries. By using a distributed ledger system, all transactions and interactions can be tracked and verified, increasing trust and accountability.
- **Pension Fund Administration**: Blockchain can provide a secure, transparent, and immutable record of all transactions related to the pension fund. This can be used to track fund allocation and distribution, ensuring that pensioners receive their due benefits and eliminating the chances of fraud.
- **Financial Management**: Blockchain can be used to create a decentralized financial system, reducing the cost and complexity of transactions. Smart contracts can automate financial operations, ensuring compliance and transparency.

Internet of Things (IoT)

CRM: IoT devices can provide real-time feedback from pensioners, helping to improve services and response times.

Pension Fund Administration: IoT devices can be used to track and monitor the health and well-being of pensioners.

Financial Management: IoT devices can be used to gather real-time financial data, helping to improve financial decision-making and risk management.

BI & Analytics, Big Data Governance & Data Science:

- **CRM:** Use BI tools for customer segmentation, behaviour analysis, and churn prediction. Big Data can help track customer interactions and analyse them for trends, sentiments, and behaviours.
- **Pension Fund Administration:** Data science and BI tools can provide visualizations of fund performance.
- **Financial Management:** Use BI and analytics for real-time reporting, trend identification, and future forecasting. Big Data governance ensures data quality and compliance.

Workflows and Orchestration layers:

- **CRM**: Workflow management tools can streamline customer service processes and improve customer experiences. Orchestration layers can synchronize data across different systems.
- **Pension Fund Administration**: Use workflows to streamline application processing, benefits calculations, and payment distributions. Orchestration layers can ensure consistency across different systems.
- **Financial Management**: Workflow tools can automate financial processes and approvals. Orchestration layers help to synchronize financial data across different systems.

Seamless Integration through ESBs (Enterprise Service Bus):

- **CRM, Pension Fund Administration, Financial Management**: ESBs can connect disparate systems, ensuring data consistency and facilitating real-time information flow between different systems. This helps to improve service delivery, fund administration, and financial management.

  The appropriate integration architecture patterns, mechanisms and technologies shall be determined for each interface.

Hubs or Central & Comprehensive API Platforms:

- **CRM, Pension Fund Administration, Financial Management**: API platforms enable the integration of different software systems. They can help connect CRM, Pension Fund, and Financial systems with other government databases for efficient data sharing.

Business Rules Engines:

- **CRM, Pension Fund Administration, Financial Management**: Business rules engines can automate decisions based on predefined rules, ensuring consistency and reducing the possibility of human error. They can be used in eligibility checks, benefit calculations, compliance checks, and risk management.

Risk Engines:

- **CRM, Pension Fund Administration, Financial Management**: Risk engines can help identify, assess, and manage risks associated with compliance, and operations. They help in optimizing portfolio risk-reward trade-offs, ensuring regulatory compliance, and enhancing operational risk management.

The use of some of these technologies would greatly improve the efficiency and effectiveness of pension fund administration, offering increased transparency, improved customer service, and better financial management. However, it is important to consider data privacy and security concerns when implementing these technologies, and to ensure compliance with all relevant regulations.

6 Integration Architecture

Integration Architecture is a strategic approach in enterprise application integration, enabling the flow of data between disparate systems and applications across an enterprise.

It provides a method for different applications to communicate and share data. This breaks down data siloes and provides visibility over application landscapes and data flows.

6.1 Integration Patterns & Types

The choice of an integration pattern depends on the specific needs and constraints of the organization, such as the existing technology stack, skill sets of the team, expected future growth, and more. Other considerations include data security, scalability, maintainability, and interoperability. The patterns can also be combined as required.

Here are some common integration architecture patterns that can be employed to achieve these goals:

Application Integration Patterns

The following are some of the integration patterns that cater for the various interfaces that apply to the solution and will be implemented based on preferred mechanism in consultation with integration partners and internal integration standards.

Real-time data request

Where data is required real-time from /by the solution using web services, microservices and APIs.

Real-time integration (via API Gateway)

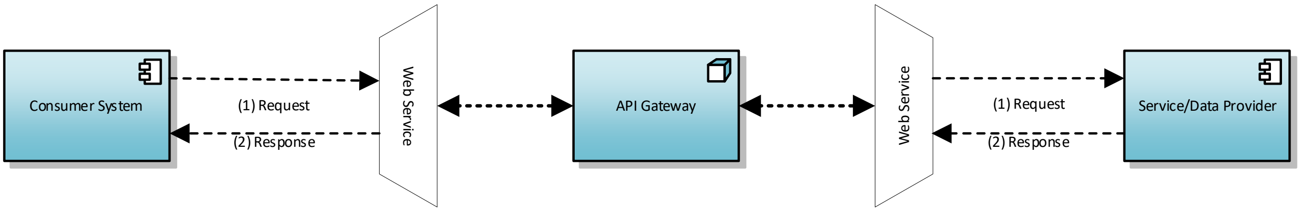
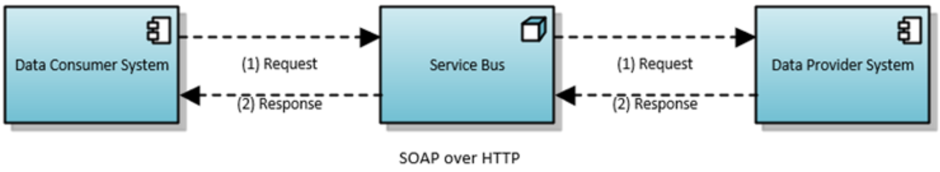


Figure 29 Real-time integration via API Gateway

Real-time integration (via ESB)

- SOAP web services via ESB



Real-time multiple data integration requests (e.g. data lookup) and then provision to consumers (via web services)

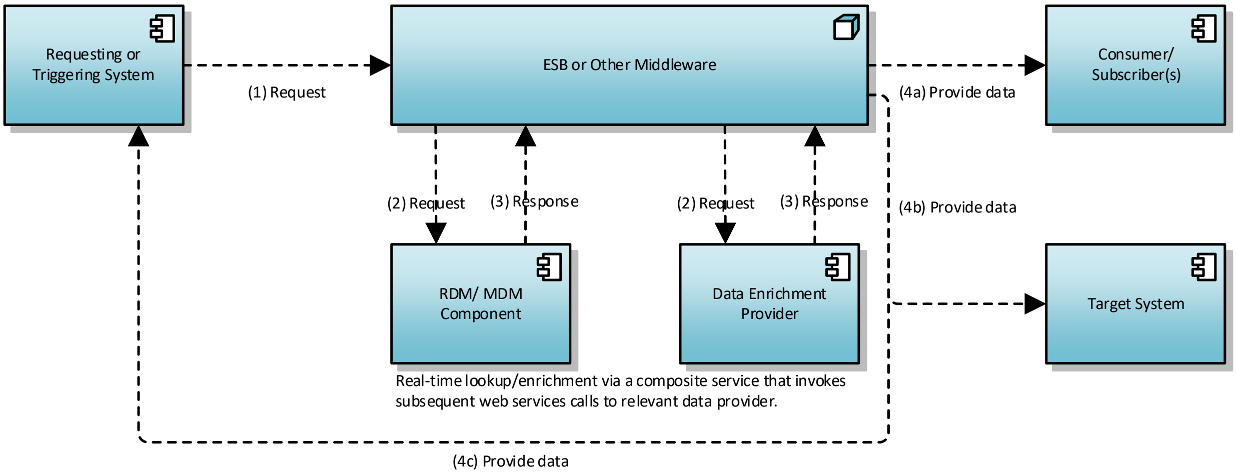


Figure 30 Real-time integration patterns

Subscriber message model: Near-Realtime data request

Where data providers can publish data and multiple consumers can subscribe to and receive the messages for consumption.
Where data is required Near-Realtime on request but no real-time synchronous response between components.

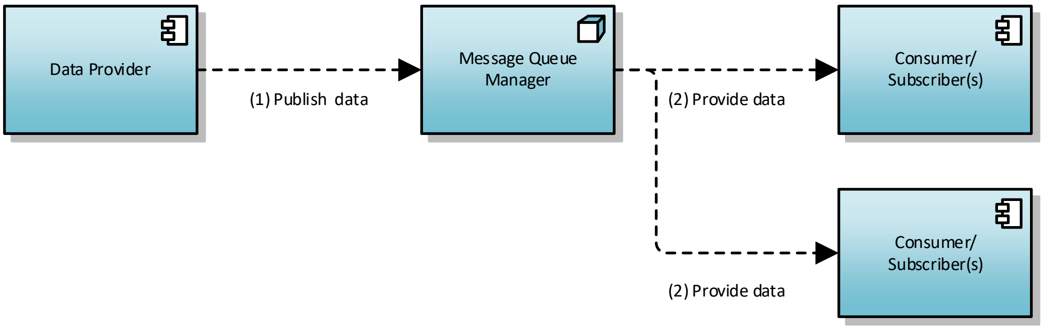


Figure 31 Subscriber message pattern

Bulk non-real-time data transfer using a batch file

Where bulk data is imported into (or from) the solution in batch files or to a secure data repository. This shall be used for use cases such as initial loads and data migration scenarios where the data might need some standardization or transformation before distribution.

Bulk data load to CDR or other Data Provisioning Repository

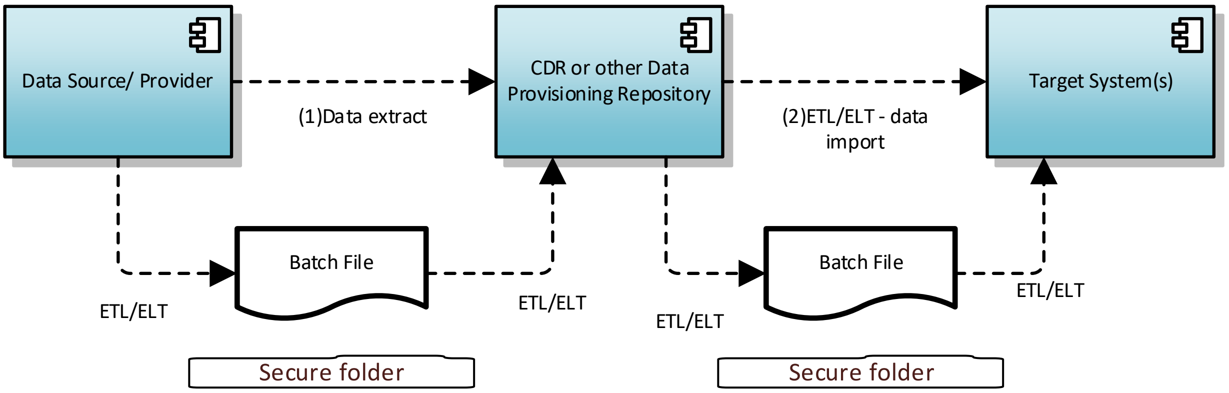


Figure 32 Bulk data using Batch file transfer pattern.

If the file is to be moved to a different location it should be transported via secure means such as SFTP over SSH.

Below is a summary of some of the standard integration patterns that can be considered for adoption.

The protocols and typical solutions are just for consideration as GPAA still needs to define the standards to be used for each integration scenario.

Hub and Spoke	
Description:	A centralized integration model where all applications connect to a central hub, which then redirects the communication to the destination application.
Technical Mechanism:	Uses a central hub as a mediator. All communications pass through the hub.
Use Cases:	Ideal for businesses with a moderate number of applications that have various integration requirements.
Benefits:	Reduces the number of direct integrations, centralizes management and monitoring.
Disadvantages:	Hub becomes a single point of failure; can be a bottleneck.
Middle-ware Components:	Integration servers, ESB (Enterprise Service Bus).
Typical Solutions:	IBM Integration Bus, MuleSoft, TIBCO.

Protocols:	HTTP(s), SOAP, REST.
Information Security Standards:	WS-Security, OAuth2, SAML

Enterprise Service Bus (ESB):	
Description:	A more evolved version of Hub & Spoke, ESB provides a set of rules and principles for integrating numerous applications together over a bus-like infrastructure.
Technical Mechanism:	Provides service orchestration, message routing, and transformation.
Use Cases:	Complex enterprises with numerous applications that require real-time integration.
Benefits:	Scalable, flexible, reduces complexity by decoupling service providers from consumers.
Disadvantages:	Can become complex and costly, potential performance overhead.
Middle-ware Components:	Messaging systems, orchestration engines.
Typical Solutions:	Apache Camel, WSO2 ESB, JBoss Fuse.
Protocols:	SOAP, REST, JMS.
Information Security Standards:	WS-Security, OAuth2, SAML2.

Point-to-Point	
Description:	Direct integration between two applications without any middle layer.
Technical Mechanism:	Direct API calls or database connections between systems.
Use Cases:	Simple integration requirements with very few systems.
Benefits:	Simple, often faster due to direct connections.
Disadvantages:	Not scalable, increases complexity as more systems are added.

Middle-ware Components:	Direct APIs, database connectors.
Typical Solutions:	JDBC connections, direct web service calls.
Protocols:	HTTP(s), JDBC, ODBC.
Information Security Standards:	SSL/TLS, API Keys.

Microservices Architecture	
Description:	Decompose an application into loosely coupled services that operate independently.
Technical Mechanism:	Each service operates independently, communicates via lightweight protocols.
Use Cases:	Complex systems that require scalability, agility, and maintainability.
Benefits:	Scalability, resilience, and technological freedom.
Disadvantages:	Can introduce complexity in terms of management and monitoring, potential for data inconsistency.
Middle-ware Components:	Service discovery, API gateways.
Typical Solutions:	Kubernetes, Docker, Istio.
Protocols:	REST, gRPC, GraphQL, REST API and Service mesh
Information Security Standards:	JWT, OAuth2.

Message Queue	
Description:	Allows applications to communicate by sending messages to each other.
Technical Mechanism:	Asynchronous messaging.
Use Cases:	Decoupling producers and consumers; Load leveling.
Benefits:	Scalability; Decoupling; Resilience.

Disadvantages:	Message order not guaranteed; Monitoring required.
Middle-ware Components:	Message Queue software.
Typical Solutions:	Servers or cloud platforms for the queue.
Protocols:	RabbitMQ, Apache Kafka, AWS SQS.
Information Security Standards:	AMQP, MQTT, STOMP.

Hybrid Integration	
Description:	Combines multiple integration patterns. Combines real-time and batch integrations. Some operations might be carried out in real-time, while others are batch processed.
Technical Mechanism:	Combines APIs, ESBs, Message Queues, etc.
Use Cases:	Enterprises with varied requirements; Cloud and on-premises integration. Useful for scenarios where some data is needed immediately, while other data can be processed at a later time.
Benefits:	Flexibility; Best of different patterns.
Disadvantages:	Complexity; Requires skilled architects.
Middle-ware Components:	Varied
Typical Solutions:	Tailored to specific needs.
Protocols:	Multiple.
Information Security Standards:	Comprehensive based on needs.

API Gateway	

Description:	A server that acts as an API front-end, receiving API requests, enforcing throttling and security policies, passing requests to the back-end service, and then passing the response back to the requester.
Technical Mechanism:	Acts as a reverse proxy to accept all application requests and route requests to the appropriate service.
Use Cases:	Microservices architectures, mobile applications.
Benefits:	Centralized management, security enforcement, analytics and monitoring.
Disadvantages:	Can introduce a single point of failure.
Middle-ware Components:	Reverse proxy, request/response transformers.
Typical Solutions:	Amazon API Gateway, Kong, WSO2 API Manager.
Protocols:	REST, GraphQL , WebSocket.
Information Security Standards:	OAuth, JWT, API Keys.

Data Integration	
Description:	Focuses on the consistent access and delivery of data across the spectrum of data subject areas. Combines data from different sources to provide a unified view or dataset. Can include data merges data from different databases, ensuring that they can communicate and share information.
Technical Mechanism:	ETL (Extract, Transform, Load) processes, real-time data synchronization. Database level integration can involve techniques such as database replication, federation, or warehousing.
Use Cases:	Data warehousing, data lakes, analytics.
Benefits:	Unified view of data, supports decision-making.
Disadvantages:	Can be resource-intensive, needs proper data governance.
Middle-ware Components:	ETL tools, data connectors.
Typical Solutions:	Apache Nifi, Talend, Informatica.

Protocols:	SQL, NoSQL.
Information Security Standards:	Data encryption, data masking.

6.2 Standard Integration Interface Types

Integration interfaces enable different systems, applications, or components to work together and communicate with one another. These interfaces should be implemented in accordance with the integration patterns.

Each of these interfaces can be chosen based on the requirements such as complexity, scalability, security, and the type of data being exchanged.

Below are some common integration interface types:

API (Application Programming Interface):	• **REST (Representational State Transfer)**: It uses HTTP methods and a stateless, client-server architecture. • **SOAP (Simple Object Access Protocol)**: It relies on XML for its message format and is typically more rigid than REST. • **GraphQL**: It allows the client to request only the data it needs, providing more flexibility and efficiency. • **gRPC**: Utilizes HTTP/2 for transport and Protocol Buffers as the interface description language, enabling more efficient communication.
File-Based Interfaces:	• **CSV, XML, JSON files**: Systems can share these common file formats to transfer data.
Database Interfaces:	• Directly connecting to databases (e.g., SQL, NoSQL) to access or manipulate data.
Webhooks:	• Allow systems to send real-time data to other systems when certain events occur.
Middleware Integration:	• **ESB (Enterprise Service Bus)**: A software architecture that enables communication among various applications. • **Message Queues**: Such as RabbitMQ or Kafka, they allow asynchronous data passing between applications.
Custom Interfaces:	• Sometimes, specialized integration might require custom coding or specific interfaces designed for the purpose.

Frontend Integration:	• **IFrames**: Embedding one webpage within another. • **Web Components**: Reusable custom elements that can be used across different web applications.
Hardware Interfaces:	• Integration at the hardware level, such as GPIO in embedded systems.
Cloud Integration Services:	• Platforms like AWS, Azure, or GCP offer various services and tools for integration across applications, data, and processes.
Service Mesh:	• Such as Istio, it controls how different parts of an application share data with one another.
Batch Integration:	• Scheduled data transfer at specific intervals, usually involving large volumes of data.
Real-time Integration:	• Provides immediate data transfer and synchronization between systems.
Remote Procedure Call (RPC):	• Allows a program to cause a procedure (subroutine) to execute in another address space (commonly on another server).
EDI (Electronic Data Interchange):	• Standardized formats for exchanging business data.
IoT (Internet of Things) Integration:	• Interfaces specifically designed to connect IoT devices and systems.
Content Integration:	• Tools and systems that enable content from various sources to be accessed, searched, and worked with through a single interface.

6.3 Integration Solutions Landscape

Current Integration Solutions

GPAA has the following integration solutions.

Platform/ Solution	Usage & Purpose	Target State Considerations
Oracle Service Bus (OSB)	Oracle Service Bus (OSB) is an Enterprise Service Bus. transforms complex and brittle architectures into agile integration networks by connecting, virtualizing, and managing interactions between services and applications.	To be reviewed to determine if relevant for future integration. This might be decommissioned.

Oracle JMS	Messaging/Queue based integration.	Can be utilized in specific use cases, including when you only need to process a small number of messages per day.
API Gateway	API Integration management. An API Gateway is used as the entry point for client requests to an API.	Strategic fit
Oracle SOA Suite	A hot-pluggable software suite that enables you to build, deploy, and manage integrations using service-oriented architecture (SOA). This enables the set up, management and orchestration of services into composite applications and business processes.	To be assessed for strategic fit.
Connect:Direct	Provides security-hardened, point-to-point file transfers.	TBA
TotemoData	Secure Managed File Transfer	TBA

6.4 Considerations

It is important to consider various factors such as data security, scalability, maintainability, and interoperability.

Security Considerations:

1. **Authentication and Authorization**: Ensure only authorized entities can access your systems.
2. **Data Encryption**: Both in-transit and at-rest to ensure data privacy and security.
3. **Rate Limiting**: For APIs, to prevent abuse and overloading.
4. **Monitoring and Logging**: To detect and respond to potential security threats.

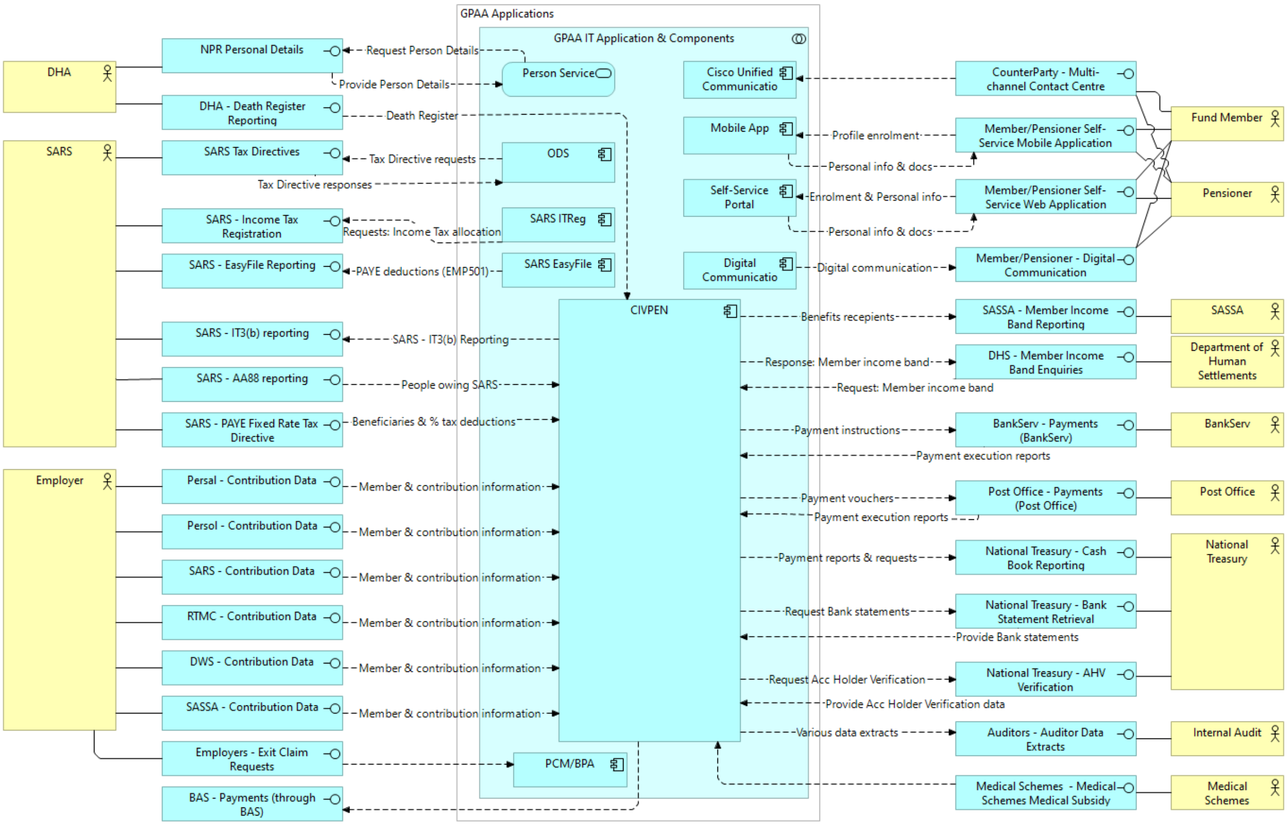
Operational Considerations:

1. **Monitoring**: Use tools to monitor system health, traffic loads, and error rates.

2. **Scalability**: Ensure the architecture can handle the expected load and can be scaled up or down as needed.
3. **Maintainability**: Make sure the architecture is manageable, upgradable, and adaptable.

6.5 External Interfaces

GPAA has several interfaces that enable data exchange and interaction with third parties at a system level. The diagram below shows some of the current key external interfaces. These shall need to be retained and enhanced in the implementation of the Modernisation Programme.



GPAA Applications
GPAA IT Application & Components
DHA
SARS
Employer
NPR Personal Details
DHA - Death Register Reporting
SARS Tax Directives
SARS - Income Tax Registration
SARS - EasyFile Reporting
SARS - IT3(b) reporting
SARS - AA88 reporting
SARS - PAYE Fixed Rate Tax Directive
Persal - Contribution Data
Persol - Contribution Data
SARS - Contribution Data
RTMC - Contribution Data
DWS - Contribution Data
SASSA - Contribution Data
Employers - Exit Claim Requests
BAS - Payments (through BAS)
Request Person Details
Provide Person Details
Death Register
Tax Directive requests
Tax Directive responses
Requests: Income Tax allocation
PAYE deductions (EMP501)
SARS - IT3(b) Reporting
People owing SARS
Beneficiaries & % tax deductions
Member & contribution information
Person Service
ODS
SARS ITReg
SARS EasyFile
CIVPEN
PCM/BPA
Cisco Unified Communicatio
Mobile App
Self-Service Portal
Digital Communicatio
Profile enrolment
Personal info & docs
Enrolment & Personal info
Personal info & docs
Digital communication
Benefits recepients
Response: Member income band
Request: Member income band
Payment instructions
Payment execution reports
Payment vouchers
Payment execution reports
Payment reports & requests
Request Bank statements
Provide Bank statements
Request Acc Holder Verification
Provide Acc Holder Verification data
Various data extracts
CounterParty - Multi-channel Contact Centre
Member/Pensioner Self-Service Mobile Application
Member/Pensioner Self-Service Web Application
Member/Pensioner - Digital Communication
SASSA - Member Income Band Reporting
DHS - Member Income Band Enquiries
BankServ - Payments (BankServ)
Post Office - Payments (Post Office)
National Treasury - Cash Book Reporting
National Treasury - Bank Statement Retrieval
National Treasury - AHV Verification
Auditors - Auditor Data Extracts
Medical Schemes - Medical Schemes Medical Subsidy
Fund Member
Pensioner
SASSA
Department of Human Settlements
BankServ
Post Office
National Treasury
Internal Audit
Medical Schemes

Figure 33 GPAA External Third-Party Interfaces

Below are the interfaces shown in the diagram above.

Interface Name	Description	Interface Type	GPAA Application	Security Measure
National Population Register (NPR)	Population register regarding South African	SOAP	Person Service	TLS/SSL Encryption

	Citizens/Permanent Residents			
Tax Directives	Requests/Responses to/from SARS regarding Tax Directives	Text Files/ Fixed length fields	ODS/Tax Directives	SSH Encryption
Income Tax Registration	A facility provided by SARS to register persons for Income Tax purposes	Text Files/ Fixed length fields	ITReg	Unknown
EasyFile Reporting	A facility provided by SARS for employers to submit reports of PAYE deductions of their emplyees	Text Files/ Fixed length fields	EasyFile	Unknown
IT3(b) reporting	A facility to report interest paid to beneficiaries twice a year	Text Files/ Fixed length fields	CIVPEN IT3(b) Reporting batch job	TLS/SSH Encryption Dual Certificates Client authentication Server Authentication
AA88 reporting	A facility enabling SARS to report to GPAA people owing SARS monies instructing GPAA to deduct money from the benefit owed to these beneficiaries and pass it over to SARS	Text Files/ Fixed length fields	CIVEPN Tax Batch job	Unknown
PAYE Fixed Rate Tax Directive	A facility allowing SARS to direct GPAA to deduct a fixed % tax rate for beneficiaries receiving income from multiple sources	Text Files/ Fixed length fields	CIVPEN Tax Batch job	Unknown

Contribution Data	The means by which employers report contribution information to GPAA	Text Files/ Fixed length fields	CIVPEN Recon	TLS/SSH Encryption Dual Certificates Client authentication Server Authentication
Contribution Data	The means by which employers report contribution information to GPAA	Text Files/ Fixed length fields	CIVPEN Recon	SSH Encryption
Contribution Data	The means by which employers report contribution information to GPAA	Text Files/ Fixed length fields	CIVPEN Recon	None
Contribution Data	The means by which employers report contribution information to GPAA	Text Files/ Fixed length fields	CIVPEN Recon	None
Contribution Data	The means by which employers report contribution information to GPAA	Text Files/ Fixed length fields	CIVPEN Recon	None
Contribution Data	The means by which employers report contribution information to GPAA	Text Files/ Fixed length fields	CIVPEN Recon	Password Protected
Payments (BankServ)	Payment instructions to BankServ for paying out benefits as well vendors	Text Files/ Fixed length fields	CIVPEN Payment Run	Hardware Encryption

Payments (Post Office)	Payment voucher information to be made to beneficiaries through Post Office branches	Text Files/ Fixed length fields	CIVPEN Payment Run	TLS/SSH Encryption Dual Certificates Client authentication Server Authentication
Cash Book Reporting	Reports to National Treasury regarding all outgoing payments. Requests to National Treasury to pay out all payments greater than R2 million.	Fixed length fields	Cash Book reporting Batch Job	PTP to SITA
Bank Statement Retrieval	Retrieval of bank account statements containing outgoing payment transactions	Fixed length fields	Bank Statement Retrieval Batch Job	PTP to SITA
AHV Verification	A mechanism for GPAA to request Account Holder Verification (AHV) and receive the results of such requests	Fixed length fields	AHV Batch Job	PTP to SITA
Member Income Band Enquiries	A mechanism that allows the Department of Human Settlements (DHS) to enquire on the income band of a person to assist in determining eligibility for housing subsidy	XML	DHS Member Income Band, CIVPEN Member Income Enquiry	IP Address filtering
Member Income Band Reporting	A mechanism to report to SASSA receivers of benefits paid out by GPAA	Fixed length fields	CIVPEN beneficiary extract batch job	SSH Encryption

Death Register Reporting	A mechanism for the Department of Home Affairs (DHA) to report the death register to GPAA so that benefit payment to deceased beneficiaries may be stopped	Text Files/ Fixed length fields	CIVPEN Death Register Processing	PTP to SITA
Auditor Data Extracts	Ad hoc Data Extracts as requested by auditors	Text Files/ Fixed length fields	Data Extract Utilities	Internal Extract
Exit Claim Requests	Requests initiated by Employers to exit members from the fund and pay them their exit benefits due	Web Application	PCM/BPA	HTTPS, User Authentication
Member/Pensioner Self-Service Web Application	A web based application allowing members/pensioners access to their data at GPAA. They can view their personal information and download various documents (e.g. benefit statement, tax documents, Payment advice)	Web Application	Self-Service Web Application	HTTPS, User registration, User Authentication, MFA
Member/Pensioner Self-Service Mobile Application	A mobile application allowing members/pensioners access to their data at GPAA. They can view their personal information and download various documents (e.g. benefit statement, tax documents, Payment advice)	Mobile Application	Self-Service Mobile Application	HTTPS, User registration, User Authentication, MFA

Digital Communication	A platform that allows the GPAA to send out communication to members/pensioners, whether it is standard communication (e.g. FundTalk, notification of out reach campaigns) or specific information to the member/pensioner (e.g. benefit statement, payment advice, tax certificates)	SMS SMTP	Digital Communications Platform	Encoded PDF files
Multi-channel Contact Centre	A facility that allows members/ pensioners/ employers to contact the GPAA and be served (hosted by In2IT)	Phone Email Fax Social networks	Cisco Unified Communications	HTTPS, User registration, User Authentication
Medical Schemes Medical Subsidy Claims	A facility to allow medical schemes to claim medical scheme subsidies for pensioners	Text Files/ Fixed length fields	CIVPEN Medical Scheme processing batch job	TLS/SSH Encryption Dual Certificates Client authentication Server Authentication
Payments (through BAS)	A facility provided by BAS to pay out Military Medical Claims	Text Files/ Fixed length fields	CIVPEN Military Medical Claim Payment batch job	User ID/Password PTP to SITA

7 Security Architecture

7.1 Information Security Strategy Overview

Information Security Framework

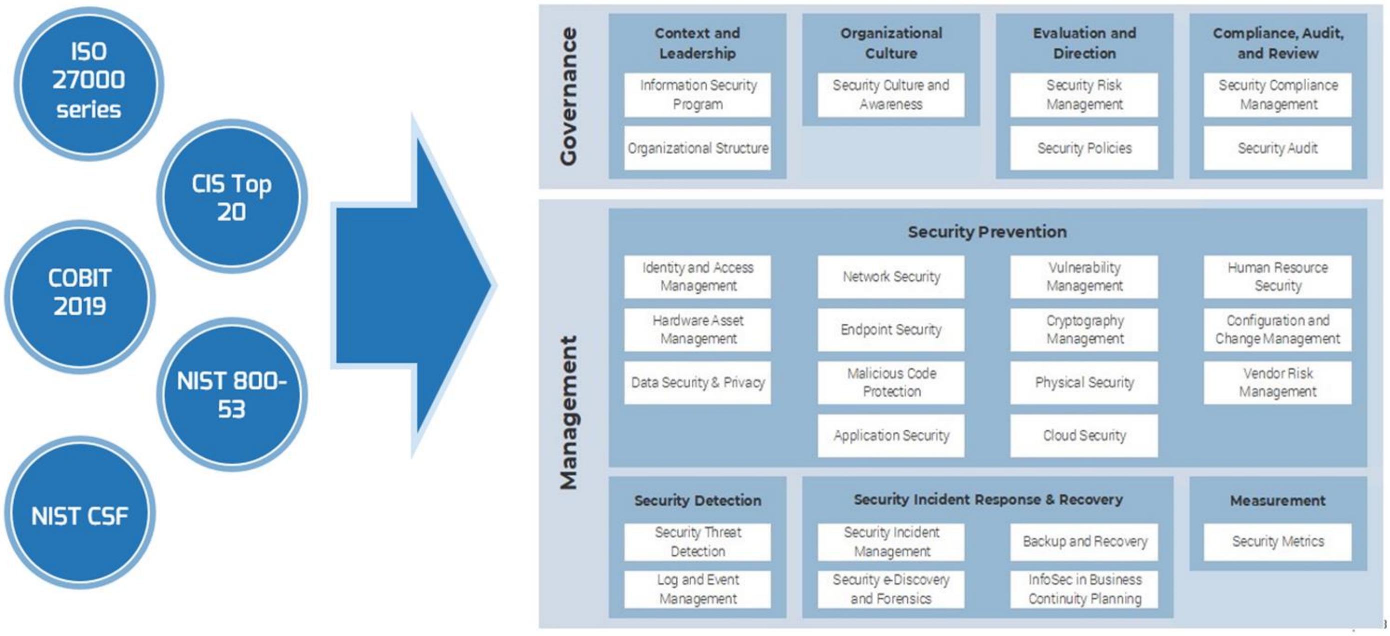


Figure 34 GPAA Information Security Framework

GPAA has adopted Infosec's Information Security Framework was for risk assessments and the determination of security controls and programs. The following control, program, and risk frameworks have been incorporated:

- National Institute of Standards and Technology (NIST) 800 series
- NIST Cybersecurity Framework (CFS)
- International Organisation of Standards (ISO) 27001
- Centre for Internet Security (CIS) Critical Security Controls
- COBIT 2019

Dealing with Components of the Security Framework

To address the components of Information Security Governance as part of the Information Security Framework above, it's essential to consider both the Information Security Architecture and the broader Enterprise Architecture. The table below describes how the Enterprise and Security

Architectures can support the Information Security Strategy and the Security Strategy through dealing with the various framework components.

Information Security Governance components

Component	Information Security Architecture	Enterprise Architecture
Information Security Program	Develop a comprehensive program that includes detailed security strategies, plans, and objectives aligned with the organization's risk profile.	Integrate the security program with the overall enterprise strategy, ensuring it supports business goals and objectives.
Organizational Structure	Define a clear structure for the security team, including roles and responsibilities. Ensure alignment with IT and other business units.	Design the organizational structure to facilitate effective communication and collaboration between departments on security matters.
Security Culture and Awareness	Implement ongoing training and awareness programs. Promote a culture of security mindfulness among all employees.	Embed a security-first mindset in the organization's culture, ensuring it permeates all levels and departments.
Security Risk Management	Conduct regular risk assessments. Implement a risk management process that identifies, analyses, and mitigates information security risks.	Align risk management with the enterprise's risk framework, ensuring consistency in how risks are managed across the organization.
Security Policies	Develop and maintain comprehensive security policies that address various aspects like access control, data protection, incident response, etc.	Ensure that security policies are well integrated with business policies, reflecting a unified approach to governance.
Security Compliance, Audit, & Review	Regularly perform internal and external audits. Ensure compliance with legal, regulatory, and industry standards. Review and update security measures.	Integrate compliance and audit processes with enterprise governance structures. Regularly review and adapt to changing regulations and standards.

Information Security Management components

Component	Information Security Architecture	Enterprise Architecture
Security Prevention	Implement layered security measures, including firewalls, intrusion detection systems, and security policies.	Align prevention strategies with organizational objectives and IT infrastructure.
Identity & Access Management	Deploy IAM solutions for secure access control, including multi-factor authentication and role-based access.	Integrate IAM across all systems and applications, ensuring a unified approach to access management.
Hardware Asset Management	Maintain an inventory of all hardware assets. Implement security controls on all devices.	Incorporate hardware asset management into the overall IT management strategy, ensuring compatibility and compliance.
Data Security & Privacy	Enforce data encryption, classification, and privacy policies.	Ensure data security is embedded in the data lifecycle processes across the organization.
Network Security	Utilize network segmentation, firewalls, and secure VPNs to protect the network.	Design a network architecture that supports robust security measures.
Endpoint Security	Deploy anti-malware, endpoint detection and response systems, and ensure secure device configurations.	Integrate endpoint security into the overall IT landscape, ensuring consistency across devices.
Malicious Code Protection	Implement anti-malware solutions and regularly update them.	Coordinate with software management to ensure all applications and systems are protected against malicious code.
Application Security	Enforce secure coding practices, use WAFs, and conduct regular security assessments.	Align application development with security standards and best practices.
Vulnerability Management	Regularly perform vulnerability scans and remediate identified vulnerabilities.	Integrate vulnerability management into software and infrastructure lifecycles.

Cryptography Management	Manage cryptographic keys effectively and ensure encryption algorithms are up-to-date.	Ensure cryptography is consistently implemented across the IT environment.
Physical Security	Secure physical access to critical infrastructure and data centres.	Incorporate physical security considerations into the design and layout of facilities.
Cloud Security	Implement security controls in cloud environments, including CSPM tools.	Develop a cloud strategy that includes security as a core component.
Human Resource Security	Conduct background checks, provide security training, and enforce security policies from onboarding to offboarding.	Integrate security considerations into HR processes and policies.
Configuration & Change Management	Establish processes for securely managing changes in the IT environment.	Align change management processes with broader organizational objectives and IT strategies.
Vendor Risk Management	Assess and manage the security risks associated with third-party vendors.	Integrate vendor risk management into the procurement and contract management processes.
Security Threat Detection	Implement systems for continuous monitoring and detection of security threats.	Align threat detection tools and practices with the overall IT and business strategy.
Log and Event Management	Use SIEM tools for centralized log collection, monitoring, and analysis.	Ensure log management is integrated with IT operations and incident response processes.
Security Incident Response & Recovery	Develop and test incident response and recovery plans.	Integrate incident response and recovery into the overall business continuity and crisis management plans.
Security Incident Management	Establish processes for effective handling and reporting of security incidents.	Embed incident management into organizational processes, ensuring clear communication and coordination.
Security e-Discovery & Forensics	Implement tools and processes for electronic discovery and forensic	Ensure e-discovery and forensic capabilities are aligned with legal and compliance requirements.

	analysis in case of security incidents.	
Backup & Recovery	Regularly backup critical data and test recovery procedures.	Integrate backup and recovery into the overall IT and business continuity planning.
Business Continuity & Planning	Develop and maintain a business continuity plan that includes IT systems and data.	Align business continuity plans with organizational objectives and risk management strategies.
Measurement & Metrics	Implement KPIs and metrics to measure the effectiveness of security controls and report to management.	Align security metrics with broader organizational performance metrics and objectives.

It is essential for the organization to not only establish these components but also to ensure they are dynamically updated and responsive to the changing landscape of information security threats and challenges.

Regular review, updates, and stakeholder engagement across these areas are critical for maintaining a robust information security posture.

Effective communication and collaboration between the Information Security team and other business units are essential to ensure a holistic and integrated approach to Information Security

Current State Analysis

Risk Assessment

A security risk assessment was conducted for the Department and the security risk assessment is influenced by risk factors of threats, assets, incidents, and vulnerabilities from people, systems, and supply chains. The risk level was assessed as high and depicted in the figure below.

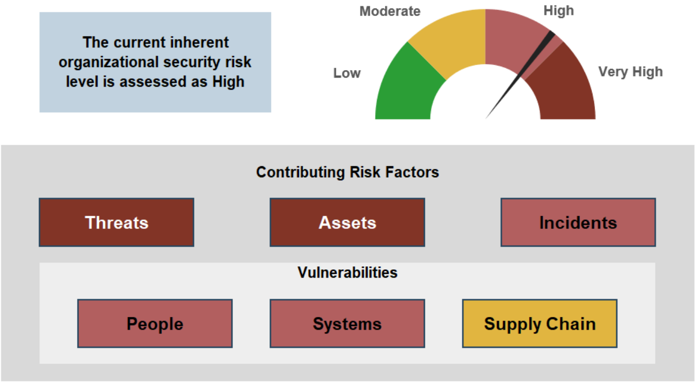

The current inherent organizational security risk level is assessed as High
Moderate
High
Low
Very High
Contributing Risk Factors
Threats
Assets
Incidents
Vulnerabilities
People
Systems
Supply Chain

Figure 35 Current state security risk assessment

The Pressure Analysis

The Departments must comply with laws and regulations & oversight requirements.

- The privacy laws,
- National Security Standards,
- Public Service Security Directives, and
- applicable industry standards for risk and security.

They include:

- POPIA,
- the Minimum Information Security Standard (MISS), and
- the Public Service Information Security Directive.

Also, there are contractual requirements by the GEPF that the GPAA must meet. The pressure analysis level was assessed as high and depicted in the figure below.

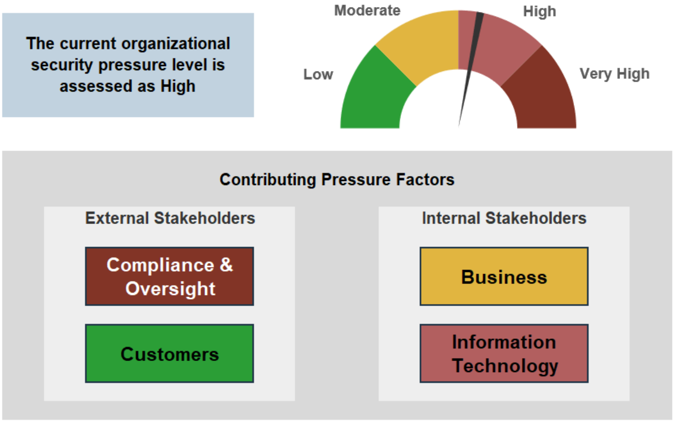


Figure 36 Current state Security pressure assessment

The Target State Vision

The Information Security Target State is measured by a common maturity model with a scale of 1 being Ad-hoc and 5 being Optimised and is calculated from the security risk assessment and pressure analysis. The target state for information security is assessed on a scale of 3.6. and this is the desired target state.

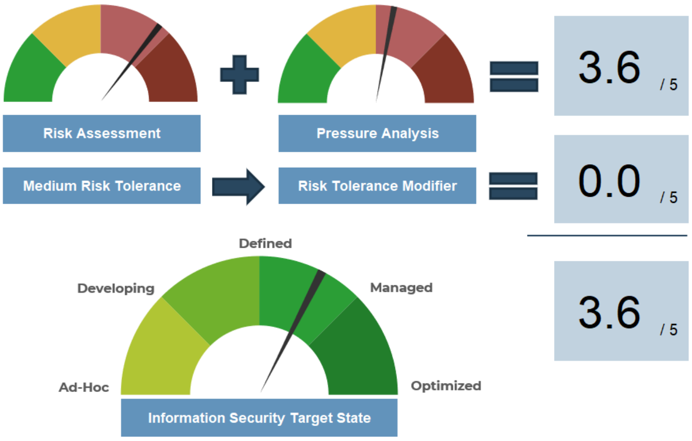


Figure 37 Desired Security Target State

GAP Assessment

The figure below is a visual representation of the gaps in the security domains between the current state and the desired state. The colour codes indicate the difference between the information security domains of the current and desired state;

- green indicates that the gap is extremely low,
- orange indicates that the gap is medium, and
- red indicates that the gap is high.

Domains without colour indicate that they are not applicable or not assessed.

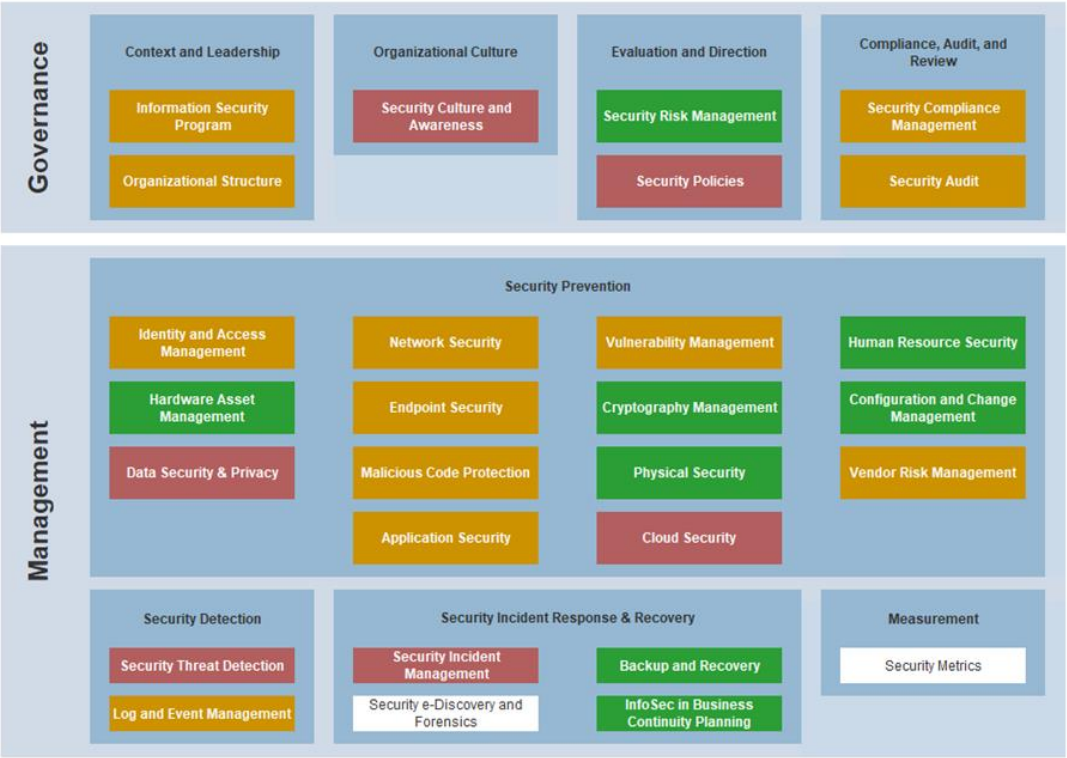


Figure 38 Gaps in the security domains between the current state and the desired state

Information Security Strategic Considerations

The Security Architecture outlines various aspects that need to be incorporated in the Taret Security Architecture.

Security Compliance Management

The Department is required to comply with laws, regulations, and standards. These include data privacy and security laws such as POPIA, National security standards such as the Minimum Information Security Standards, and directives from the National Department of Public Administration such as the Information Security & the Cloud Computing Directives. All of these and other security compliance requirements applicable are considered in the implementation of security controls

There are also security requirements in the agreements with shareholders. These requirements included bi-annual Pentests to business-critical applications and remedial of any shortcomings, and this is to ensure that the computing environment is secure.

Security Audit

While the auditing findings are tracked in the audit register, Information Security findings will be prioritised and corrected. An appropriate and acceptable action plan will be developed, and the plan will be executed accordingly.

Identity and Access Management

With ever-evolving and increasing cyber attacks and cyber threats targeting privileged accounts, modern forms of authentication are required, and amongst them are Multifactor Authentication and Just in Time access. Information security policies will direct the use of modern forms of authentication for access to all ICT infrastructure assets.

A Privileged Access Management (PAM) solution is required, and Information Security Directorate will look to implement the solution to help secure and manage access to the Department's ICT infrastructure, Applications, and Data. The PAM solution will ensure that local admin accounts, domain admins, critical service accounts, and applications accounts are centrally managed as well as ensuring that the various security management and regulatory requirements are met for these accounts.

Data Security & Privacy

The Minimum Information Security Standard is the overarching standard that defines data classification requirements. Also, the Department collects, processes, and stores personally-identifying and finance-related information and these are regulated by laws and industry standards requiring the Department to comply with these laws and standards. To date, employee computers are encrypted for data protection when laptops are lost regardless of the sensitivity of the data on the device or the access of the owner of the device.

However Data belong to the business, and it must decide its classification or sensitivity level; so the GPAA business, with assistance from ICT, will embark on tasks and initiatives that ensure that are appropriate policies for data classification and sensitivity levels, data discovery solutions, data management solution, and data security, and data loss prevention solutions that ensure that the critical business information is safeguarded accordingly to its classification or sensitivity requirement. This will also apply to the data in the cloud.

Network Security

Securing ICT infrastructure is a priority. There are initiatives underway to procure and install Next Generation Firewall to replace the old firewall devices. Information Security is also looking to deploy Network Detection and Response (NDR) solutions. NDR solutions analyse network traffic to detect malicious activity inside the perimeter (east-west) and support intelligent threat detection, investigation, and response. NDR, like EDR, can stop an attack that is in progress before it causes more damage. In addition, Network Intrusion Detection and Network Prevent solutions will also be deployed to detect and prevent intrusion

Email Security

A cloud email security gateway will be implemented to replace the current on-premises and outdated email gateway. The cloud gateway solution offers advanced email security features to detect and prevent recent and advanced email threats including brand protection. The solution will also be including an email archiving solution to resolve the current email archiving challenges in the Department. The cloud solution will comply with ISO standards of security and privacy to ensure that the GPAA information is secured

Endpoint Security

Information security will continue to develop new security baseline configuration documents or standards to harden operating systems and applications while achieving a balance between operational functionality and security. These standards will set the minimum-security control configuration required to securely configure ICT assets. The overarching configuration standards will be from the CIS benchmarks and where necessary consideration will also be made for baseline security configuration by software vendors. The CIS will help to achieve compliance with industry regulations and improve cyber hygiene from poor configurations.

Cloud Security

A Cloud Access Security Broker (CASB) will be implemented to provide secure connections, policy enforcement, threat protection, and data security among others between the Department and the cloud provider.

The GPAA will utilise a cloud service provider and the majority of the responsibility for security will be included in the managed service.

Mobile Device Management

A Mobile Device Management solution is required to manage and control Departmental information that is or could be processed and stored by these mobile devices.

A0 Mobile Device Management policy must be in place to direct the use of mobile devices in the Department.

Applications Security

One of GPAA's strategic thrusts is the retirement of legacy applications. Legacy applications are a risk and could be easily exploited by cybercriminals to gain unauthorised access. Also, the applications cannot comply with current security requirements nor meet industry standards leading to security audit findings that cannot be resolved because of unsupported software. For such applications, the GPAA will start initiatives and tasks to replace the applications.

The GPAA has developed its applications in the past. Should this trend continue, a code assessment tool for static code analysis will be used to identify security vulnerabilities in the code early in the development process.

Continuous Vulnerability Management

The goal of vulnerability assessment is to highlight issues before they are purposefully or inadvertently used to compromise ICT assets. The Information security directorate will continue to implement and improve measures to identify, assess, remediate, or mitigate (i.e. Configuration Baseline, Hardening, Patching, or Compensating Controls), and validate the remediations or mitigations. The Vulnerability Management process will be reviewed and updated to ensure that vulnerabilities are managed in a manner that does not expose the Department to threats.

Database Security Assessment & Activity Monitoring

Security configuration scanning and knowing where sensitive data resides is an essential part of regulatory compliance. A DBSAT can analyse database security configuration and monitor unusual or unauthorised activities independently from the database audit logs. The solution can be used whether databases run on-premises or in Cloud Services. With cloud migration on the Horizon, it is important to ensure that databases are configured securely, audit logs are monitored, and the data’s sensitivity or classification level in the database is known. DBSAT will also resolve the current database auditing and monitoring challenges.

Threat Detection and Response

The Security Operations Center (SOC) and Endpoint Detection and Response (EDR) will be implemented to monitor, detect, and respond to cyber threats quickly. This will be achieved through managed security service.

Key functions of a SOC solutions may include:

- Real-time monitoring of network and system activities.
- Incident detection and response.
- Threat intelligence gathering and analysis.
- Incident investigation and analysis.
- Forensics and digital evidence collection.
- Coordination with various departments to mitigate security risks.
- Developing and implementing security policies and procedures.

Key features of EDR solutions may include:

- Real-time monitoring of endpoint activities and behaviour.
- Detection of suspicious or malicious activities.
- Rapid incident response and containment at the endpoint level.
- Collecting detailed information about endpoint events for analysis.
- Behavioural analysis to identify anomalous patterns.
- Integration with threat intelligence feeds to identify known threats.
- Automation of response actions to contain threats.
- Providing security teams with visibility into endpoint incidents.

While SOC focuses on managing the overall security posture of an organization and responding to various security incidents across the network, EDR specifically addresses threats targeting individual devices and endpoints. These two concepts often work together, as EDR solutions feed endpoint data and alerts to the SOC for further analysis and coordination in managing broader security incidents.

7.2 Security Architecture Components

This proposed architecture leverages a layered security approach encompassing network, data, application, integration, and cloud infrastructure levels. By following industry best practices and keeping abreast of emerging threats, the organization can aim for a resilient system that supports the new CRM, Pension Administration, and Financial Management platforms while safeguarding against cyber risks.

It's crucial to note that this application architecture of the chosen platforms would need to be customized according to the specific requirements, constraints, and risk profile of GPAA, engaging on relevant configurations in cybersecurity, cloud architecture, and integration.
Ongoing monitoring, assessment, and improvement of the security measures should be an integral part of the organizational strategy to ensure continued alignment with changing business needs and technological advancements.

This architecture must align with the organizational objectives and regulatory compliance requirements while ensuring the highest level of security, data management, and integration.

7.2.1 Security Architecture Technical Framework

a. **Identity and Access Management (IAM):**

- Single Sign-On (SSO) across platforms
- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)
- Regular review and revocation of permissions

b. **Network Security:**

- Firewalls
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
- Secure VPNs for remote access
- Network segmentation
- Regular vulnerability assessments and penetration testing

c. **Data Encryption:**

- At-rest and in-transit encryption
- Key management and rotation

d. **Endpoint Security:**

- Anti-malware solutions
- Patch management
- Secure configuration

e. **Compliance and Regulations:**

- Compliance with GDPR, HIPAA, or other relevant regulatory standards
- Regular audits and monitoring
- Documentation and policies in place

7.2.2 Data Management:

a. **Data Classification and Labelling:**

- Sensitive data tagging
- Access control according to classification

b. **Data Backup and Disaster Recovery:**

- Regular backups
- Disaster recovery plans

c. **Data Integrity:**

- Checksums
- Regular data quality checks

7.2.3 Integration Architecture:

a. **Service-Oriented Architecture (SOA):**

- Standardized interfaces for service components
- Loose coupling and high cohesion for modular development

b. **Microservices:**

- Independent services for scalability
- Container orchestration (Kubernetes)

c. **API Gateways:**

- Centralized control and security

- Rate limiting, logging, and monitoring

7.2.4 Application Security:

- DevSecOps
  - Secure coding practices
  - Regular code reviews
- Web Application Firewalls (WAF)
- OWASP Top 10 mitigations

7.2.5 Cloud Infrastructure:

- Selection of reputed Cloud Service Providers (CSP) with necessary certifications
- Implementing Cloud Security Posture Management (CSPM)
- Secure cloud configuration and continuous monitoring
- Hybrid or Multi-cloud strategy as needed for redundancy and scalability

7.3 Directives and Standards:

There are various directives and standards stated for compliance, and these overlap in their goals and requirements. Therefore, integrating them into one cohesive strategy, as was done on the Information Security Strategy, can streamline compliance efforts.

Proposal for Integration:

- Develop a unified compliance framework where common requirements from each directive and standard are identified and mapped to specific controls. This would reduce redundancy and ensure a comprehensive approach.
- Utilize GRC (Governance, Risk Management, and Compliance) tools to track and report on compliance across multiple standards.

In essence, while each directive and standard has its unique emphasis, they all share the common goal of enhancing cybersecurity within the organization. Continuous alignment of the organization's security strategies with these directives will provide a holistic and multi-faceted defence against cyber threats while ensuring adherence to regulatory and industry best practices.

8 Technology Architecture

8.1 Current State Overview

The GPAA has a single primary Data Centre (onsite) and a secondary site with appropriate environmental, physical and security controls supporting access to both onsite and remote workers.

Both Data Centres host virtual environments (for Servers), resulting in low physical space requirements and power consumption.

The following is a summary of some of the GPAA infrastructure Architecture elements.

8.1.1 Hardware & Infrastructure

GPAA maintains three sets of hardware architectures, each with its own set of servers, storage, and administration services.

These hardware architectures are:

- **IBM Mainframe**
  This is running the CIVPEN application. This is owned and hosted at GPAA and administered by third-party organisations. The Mainframe runs its own servers, storage and internal network. It is connected via a one GByte network interface to the other servers in the organisation.
  Backups are performed on the Mainframe separately to the standard backup facility that is used at GPAA.

- **Oracle SuperCluster**
  This is running the Oracle Fusion Stack, Oracle Database, and related applications like the PCM/BPA and related / similar applications.
  GPAA has two Oracle SuperCluster half-racks for the two data centres it manages: Hamilton data centre and Gallo Manor datacentre.
  GPAA is also in the process of implementing Identity & Access Management (IAM), Enterprise Content Management (ECM) and the Scanning & Indexing business process on the SuperCluster systems.
  Following evaluation and confirmation by Oracle, or an Oracle Service partner, there should be no software changes required to move applications making use of the Oracle Fusion Stack and Oracle Database, from one hardware architecture to another or to the Cloud.

- **Intel Servers** – running Microsoft servers and various Linux servers.
  Intel based servers have the largest footprint at GPAA, both at Hamilton data centre and at Gallo Manor data centre. Intel servers are used for all Microsoft applications, including domain controllers, Exchange servers, SQL Servers, SharePoint servers and more. Another area where Intel servers are used are application servers which are either Linux based or Windows Server based.
  The Intel based servers that are used at GPAA are blade servers made by HPE. The storage that is used is also made by HPE. These servers and the supporting storage are still

under support.

The hardware architecture of most cloud service providers is Intel based. As such, there is a wide range of options available for moving to cloud.

8.1.2 Software

The following tables show the key solutions that serve the capabilities in Modernisation scop, their current deployment platforms and status with regard to cloud readiness based on the Cloud Readiness Assessment previously conducted.

Pension Administration

The following applications are used for core pension administration.

Application	Description	Platform	Dependencies	Cloud Readiness	Roadmap	Risks
CIVPEN	GPAA's main application for fund administration	Mainframe, ADABAS/Natural	IBM Mainframe, Mainframe utilities (SoftwareAG products, CA Products, Adastrip, eStrip), Mainframe administration services	Limited hosting options exist in South Africa. SoftwareAG application re-hosting to a Linux (on premise or Cloud) platform exists and viable.	Rehosting target date 2025/03/31. Maintenance and enhancement until decommissioning. Modernisation programme: Fund administration activities to be migrated to a Cloud-based managed service.	Aging IBM mainframe. Availability of Adabas/Natural developers and administrators
Pekwa	Scanning & Indexing, Enterprise Content Management	Intel Servers, VB6, Oracle Database	CIVPEN, Citrix, Oracle database	Runs as a VB6 application which is unsupported by Microsoft. Not recommended for Cloud migration.	Replace with Oracle ECM and WebCenter Content. Modernisation: ECM content can be utilised / integrated with PAS	Application is running as an unsupported application which may become incompatible with current Microsoft Operating Systems at Microsoft's whim.

					Content migration timeline: 2024/3/31	
PCM/BPA	Exit Benefit Claim business process including employer steps as well as GPAA internal steps	Mainframe, Adabas/Natural, SuperCluster, Intel, Java, AngularJS	CIVPEN, Oracle Fusion Stack, KeyCloak, Pekwa	Migration from AngularJS to Angular is required prior to Cloud migration. Fusion middleware upgrade required. Workflow engine change required.	Upgrade timeline: 2023/12/31 Migration timeline: 2027/3/31 Finalise current initiatives (Contributions, Gatekeeping). Expand to cater for exit benefit claim types. Share knowledge with Pension Administration initiative projects in the Modernisation Programme	Limited developers (1 only) with PCM/BPA application knowledge.
Tax Directives (ODS)	Requests tax directives from SARS and processes responses	Intel Servers, Java, Oracle database	CIVPEN	Application written in Java but is a legacy application – rewrite recommended using current architecture in a way that it can be consumed by multiple business processes.	The application is written in a supported language and can continue being operational for the foreseeable future.	Interaction with this application cumbersome. It may hinder progress of other business processes requiring tax directives from SARS

					Rewrite timeline: 2 years / CIVPEN	
BankServ Interface	Interacts with BankServ (the banking system automated clearing bureau) for paying out benefits amounts to beneficiaries' bank accounts	Intel Servers, VB6, Oracle database	CIVPEN Prism Encryption Device.	Application written in Java but is a legacy application – rewrite recommended using current architecture in a way that it can be consumed by multiple business processes. Current BankServ Interface is dependent on a physical encryption device which is not migratable to Cloud.	The application is written in a supported language and can continue being operational for the foreseeable future. Rewrite timeline: 2 years / CIVPEN Encryption	This is a sensitive application that pay out benefits to beneficiaries. Substantial testing is required to ensure that the application is working correctly from day one to avoid over or under payments.

- **Financial Management**

The following applications are used to assist with Operational Finance. This includes all finance and accounting required to administer the various funds under GPAA's administration and the required reporting to reflect financial standing of each of the funds.

Application	Description	Platform	Dependencies	Cloud Readiness	Roadmap	Risks
CIVPEN	GPAA's main application for fund administration which includes financial management	Mainframe, ADABAS/Natural	IBM Mainframe, Mainframe utilities (SoftwareAG products, CA Products, Adastrip, eStrip), Mainframe administration services	Limited hosting options exist in South Africa. SoftwareAG application re-hosting to a Linux (on premise or Cloud) platform exists and viable.	Rehosting target date 2025/03/31. Maintenance and enhancement until decommissioning Financial management to cloud based managed services / Modernisation FMS for replacement services	Aging IBM mainframe that must either be replaced, migrated to Cloud or re-hosted on an Intel server platform. Availability of Adabas/Natural developers and administrators
Sage (AccPac)	Financial vendor management. Job costing. Some Supply Chain processes	Windows/Intel Commercial off-the-shelf software	SQL Server Integration with CIVPEN	Lift and shift is possible.	Option: Cloud migration as-is or better integrated option to other GPAA's business processes Alternative: Modernisation FMS	Moratorium on ERP software placed by National Treasury as a result of the IFMS programme

Application	Description	Platform	Dependencies	Cloud Readiness	Roadmap	Risks
BAS	A transversal system. Used for receiving various ad hoc payments from Employer government departments. Also used for paying out post-retirement medical scheme subsidies to medical schemes	Mainframe, ADABAS/Natural system owned by National Treasury. Access to the system is administered by SITA	Dependable communication to BAS	System not managed by GPAA. Cloud considerations to be made by system owner.	As informed by system owner. There are /were intentions to replace BAS by IFMS	Aging system. No GPAA control on the system. No agreed SLA. No API available, pausing challenges for seamless integration between GPAA's systems and BAS

- **Client Relationship Management (CRM)**

The following applications are being used to assist GPAA with Client Relationship Management.

Application	Description	Platform	Dependencies	Cloud Readiness	Roadmap	Risks
CIVPEN	GPAA's main application for fund administration. Includes also some aspects of Client Relationship Management	Mainframe, ADABAS/Natural	IBM Mainframe, Mainframe utilities (SoftwareAG products, CA Products, Adastrip, eStrip), Mainframe administration services	Limited hosting options exist in South Africa. SoftwareAG application re-hosting to a Linux (on premise or Cloud) platform exists and viable.	Mainframe rehosting target date 2025/03/31.	Aging IBM mainframe that must either be replaced, migrated to Cloud or re-hosted on an Intel server platform. Availability of Adabas/Natural developers and administrators
Oracle Portal General Enquiries	A web-based application used predominantly by call centre/walk-in centre agents providing a full view of the client information	Oracle Portal, Intel/Linux based, Java/JSP, Oracle database	CIVPEN	Application is running on an unsupported version of Oracle Portal – rewrite required before cloud migration or replacement with cloud ready application	This is the main CRM application currently used at GPAA, outside of self-service. **Rewrite vs Replace to be evaluated** **OR** The Modernisation programme is covering CRM aspects as one of the three pillars they are handling.	Running on an unsupported Oracle infrastructure. Failure or incompatibility issues can have detrimental affects the service levels that GPAA offers its clients which may result in reputational damage to GPAA and GEPF.

Application	Description	Platform	Dependencies	Cloud Readiness	Roadmap	Risks
Self-Service Mobile App	Self-Service facilities made available on smart phones to members and pensioners of the GEPF	Flutter/Dart, Nginx, Kubernetes/Docker, KeyCloak, Oracle Database Linux/Intel Based	CIVPEN	Cloud technologies are being used. Ready to be moved as is.	Rehosting target date 2025/12/31 Enhance services Replacement when available or Modernisation CRM	Availability of skills
Self-Service Web Application	Self-Service facilities made available as a web site to members and pensioners of the GEPF	Nginx, Kubernetes/Docker, KeyCloak, Oracle Database, Linux/Intel Based	CIVPEN	Cloud technologies are being used. Ready to be moved as is.	Rehosting target date 2025/12/31 Enhance services Replacement when available or Modernisation CRM.	Availability of skills

8.2 Target State

8.2.1 Cloud Infrastructure

The Modernisation Programme made decision to adopt a Cloud-based implementation strategy for all applications in scope. This shall come with a Managed Services approach.

The Managed Services approach when migrating to cloud-based technology typically involves a third-party provider (MSP or Managed Service Provider) overseeing, guiding, and/or executing an organization's cloud migration and ongoing management. This approach can be especially beneficial to complement in-house expertise and to allocate the internal resources to core business functions while leveraging the technical expertise of a specialized provider.

8.2.2 Considerations

There are some factors to be taken into considerations for the cloud deployments.

DPSA Cloud Directive

The South African Department of Public Service and Administration (DPSA) has gazetted a directive on cloud computing in the public service. This provides guidance to government departments and entities on how to adopt cloud computing safely and effectively. The Modernisation Programme shall need to adhere to the requirements.

The main points of the directive are:

- **Cloud Service Models**: The directive identifies the three main service models for cloud computing: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). It provides guidance on how to choose the appropriate service model based on GPAA's needs.
- **Cloud Deployment Models**: The directive also outlines the four deployment models for cloud computing: public, private, community, and hybrid clouds. It provides guidance on how to choose the appropriate deployment model based on an GPAA's security, privacy, and regulatory requirements.
- **Risk Management**: The directive emphasizes the importance of risk management when adopting cloud computing. It provides guidance on how to identify, assess, and mitigate risks associated with cloud adoption.
- **Data Protection**: The directive provides guidance on how to protect sensitive data when using cloud computing, in line with applicable legislation such as the PoPI Act and the need to keep data within the boundaries of South Africa. It emphasises the need for strong access controls, encryption, and data backup and recovery mechanisms as required from the service provider.
- **Legal and Regulatory Compliance**: The directive provides guidance on how to ensure legal and regulatory compliance when using cloud computing. It emphasises the need to comply with relevant laws and regulations, including data protection and privacy laws.

- **Service Level Agreements (SLAs)**: The directive provides guidance on how to negotiate and manage SLAs with cloud service providers. It emphasises the need to ensure that SLAs provide sufficient assurances on service availability, performance, and security while satisfying specific business requirements.
- **Vendor Management**: The directive provides guidance on how to effectively manage cloud service providers. It emphasises the need to evaluate vendors based on their security, privacy, and regulatory compliance, and to ensure that appropriate controls are in place to manage vendor risk.

GPAA Enterprise Cloud Strategy

The Modernisation Programme shall need to align to the GPAA Cloud Strategy and BAU Enterprise Cloud Architecture as this shall inform the cloud implementation and the programme can leverage off the available resources.

9 Migration Considerations

This section deals with the approach and considerations for data and applications/systems migration, particularly focussing on the methodology and approach, and NOT focussing on the planning, resourcing, change management and rollout as these will be dealt with by the relevant Programme Management teams.

The methodologies defined are not prescriptive but just provide guidance to support a logical approach and aid the associated planning. The actual migration activities and solutioning shall be dependent on the chosen solutions, the supporting vendor migration capabilities and the state of the status and readiness of the associated GPAA capabilities such as the CDR and other Data Management platforms.

9.1 Applications Migration

Migration Approach from Legacy Application to New Applications

The migration from the legacy applications to the new applications requires a well-defined and strategic approach to ensure a seamless transition of data and functionality.

The key steps in this migration approach include those below.

- **Assessment and Planning**:
  - Begin with a comprehensive assessment of the legacy applications, identifying all relevant data, processes, and dependencies.
  - Define migration objectives, including data accuracy, minimal downtime, and user training requirements.
  - Establish a project plan with clear timelines, roles, and responsibilities.

- **Data Extraction**:
  - Extract data from the legacy applications while preserving data integrity.
  - Ensure data is captured in its entirety, including historical records and metadata.
  - Verify the accuracy and completeness of the extracted data.

- **Data Transformation**:
  - Convert and transform data to meet the format and standards required by the new applications.
  - Cleanse and deduplicate data to eliminate inconsistencies.
  - Address any data quality issues and ensure data compatibility with the new environment.

- **Testing and Validation**:
  - Rigorously test the migrated data within the new applications to ensure accuracy and functionality.
  - Conduct integration testing to verify that data interactions between various modules and components are seamless.
  - Involve end-users in user acceptance testing (UAT) to validate that the new applications meet their requirements.

- **Pilot Testing**:
  - Implement a pilot phase with a subset of users to further validate the migration process and gather feedback.
  - Resolve any issues or discrepancies identified during the pilot phase.
- **Full Migration and Go-Live**:
  - Proceed with the full migration once all issues are addressed and user feedback is incorporated.
  - Plan for a coordinated Go-Live, ensuring minimal disruption to business operations.
  - Monitor the system closely during and after Go-Live to address any immediate concerns.

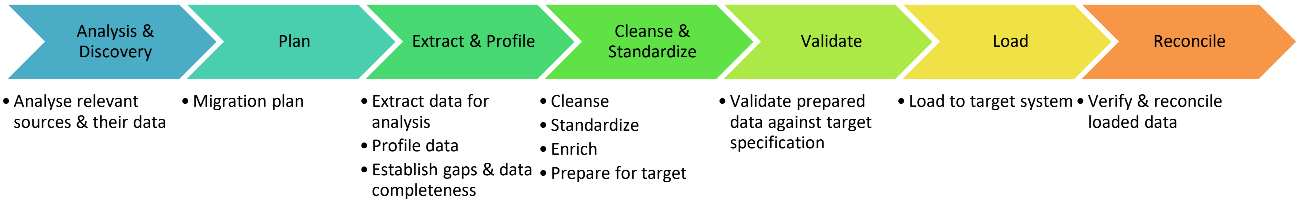
9.2 Data Migration

The Modernisation programme requires that data be migrated from the legacy applications to the target applications.

Data Migration Execution Approach

The data migration approach for transitioning from legacy applications to the new CRM, Pensions Administration System (PAS), and Financial Management System (FMS) applications encompasses a systematic and meticulous process. Beginning with a thorough understanding of source systems and data attributes, we plan and execute the migration in a logical sequence while prioritizing data integrity and quality. Data extraction, cleansing, transformation, and validation are meticulously performed before loading the data into the target systems. This approach ensures a seamless transition, ultimately leading to a successful Go-Live phase, enabling the new systems to operate efficiently with accurate and reliable data.

The basic methodology shall follow the process below.



Analysis & Discovery
- Analyse relevant sources & their data

Plan
- Migration plan

Extract & Profile
- Extract data for analysis
- Profile data
- Establish gaps & data completeness

Cleanse & Standardize
- Cleanse
- Standardize
- Enrich
- Prepare for target

Validate
- Validate prepared data against target specification

Load
- Load to target system

Reconcile
- Verify & reconcile loaded data

- **Analysis & Discovery:**
  - **Analyse Relevant Sources & Their Data:**
    - Understand the systems where data resides (Pension Administration, CRM, Financial Management Systems).
    - Review data structures, schemas, relationships, and formats.
    - Identify dependencies between datasets or applications.
    - Recognize any potential challenges or issues tied to the data or systems (e.g., proprietary formats, custom fields).
- **Plan:**
  - **Migration Plan:**
    - Define clear objectives and goals for the migration.
    - Choose the appropriate tools and technologies for data extraction, transformation, and loading.
    - Decide on the migration strategy (big bang or phased).
    - Estimate resources, timeline, and costs.
    - Determine downtime or any potential business interruptions and communicate them.
- **Extract & Profile:**
  - **Extract Data for Analysis:**
    - Use ETL tools or custom scripts to pull data from the source systems.
    - Ensure data extracted maintains its integrity and does not impact the performance of source systems.
  - **Profile Data:**
    - Generate statistics and understand characteristics of the data (e.g., distributions, value ranges, patterns).
    - Identify anomalies, outliers, or irregularities.

- **Establish Gaps & Data Completeness:**
    - Determine missing values, inconsistencies, or misalignments with the target system.
    - Understand any requirements for the new system that may not exist in the old one.

- **Cleanse & Standardize:**
    - **Cleanse:**
        - Address any anomalies, inconsistencies, or errors identified during profiling.
        - Rectify misaligned data or any corrupt entries.
    - **Standardize:**
        - Transform data into a consistent format or standard.
        - Ensure uniformity in data types, units, terms, or categorizations.
    - **Enrich:**
        - Add any missing or additional data that can enhance the quality or value of the dataset.
    - **Prepare for Target:**
        - Convert data into formats suitable for the target cloud-based system.
        - Arrange data into the structure or schema of the target system.
- **Validate:**
    - **Validate Prepared Data Against Target Specification:**
        - Ensure data conforms to the requirements, structure, and constraints of the target system.
        - Test a subset of the data in the new system to confirm alignment and compatibility.
- **Load:**
    - **Load to Target System:**
        - Use ETL tools or automated processes to move the validated data into the cloud-based system.
        - Monitor the loading process for errors or performance issues.
- **Reconcile:**
    - **Verify & Reconcile Loaded Data:**
        - Confirm that all the data in the source system has been accurately represented in the target system.

- Check data integrity, relationships, and dependencies.
- Ensure there are no missing records, duplicates, or misalignments.

9.3 Integration Interfaces Migration

Approach for Dealing with Current Integration Interfaces

Handling integration interfaces between legacy applications and the new ones is a critical aspect of a successful migration.

By following a logical approach for migration and interface management, the organization can minimize risks, ensure data accuracy, and successfully transition from legacy applications to modern ones while maintaining critical integration capabilities.

Below is an approach to address the migration:

1. **Interface Inventory**:
   - Create a comprehensive inventory of all existing integration interfaces within the legacy applications.
   - Document the purpose, data flow, protocols, and dependencies associated with each interface.
2. **Analysis and Mapping**:
   - Analyse each integration interface to understand its role in the business processes.
   - Identify the corresponding interfaces or APIs in the new applications.
   - Create a mapping document that outlines how data and processes will transition from old to new interfaces.
3. **Interface Redesign**:
   - Redesign and redevelop integration interfaces to align with the architecture and protocols of the new applications.
   - Ensure that data mappings, transformations, and data flow are consistent with the new system's requirements.
4. **Testing and Validation**:
   - Thoroughly test the redesigned integration interfaces to ensure data consistency and reliability.

- Conduct end-to-end testing to verify that data exchange between legacy and new systems is seamless.

5. **Parallel Operations**:

   - During the migration, maintain parallel operations of both the legacy and new interfaces to validate data consistency and integrity.
   - Monitor data flows and troubleshoot any discrepancies promptly.

6. **Switch-Over**:

   - Coordinate the switch-over from the legacy interfaces to the new ones during the Go-Live phase.
   - Ensure minimal downtime and a smooth transition.

10 Enterprise Architecture Governance Considerations

10.1 The Current ICT Governance Framework

The DPSA's CGICTPF is influenced by the following international best practices, namely:

- ISO/IEC 38500,
- King III commission recommendations,
- COBIT®5 and
- ITIL frameworks.

The GPAA ICT governance structure can be depicted at a high level by the ICT Governance Structure diagram below. The Department of Public Service and Administration (DPSA) developed the Corporate Governance of ICT Policy Framework (CGICTPF) for adoption by departments.

The CGICTPF has now evolved to recommend governance structures in government departments. The recommendations of the CGICTPF were examined and applied to the GPAA ICT governance framework.

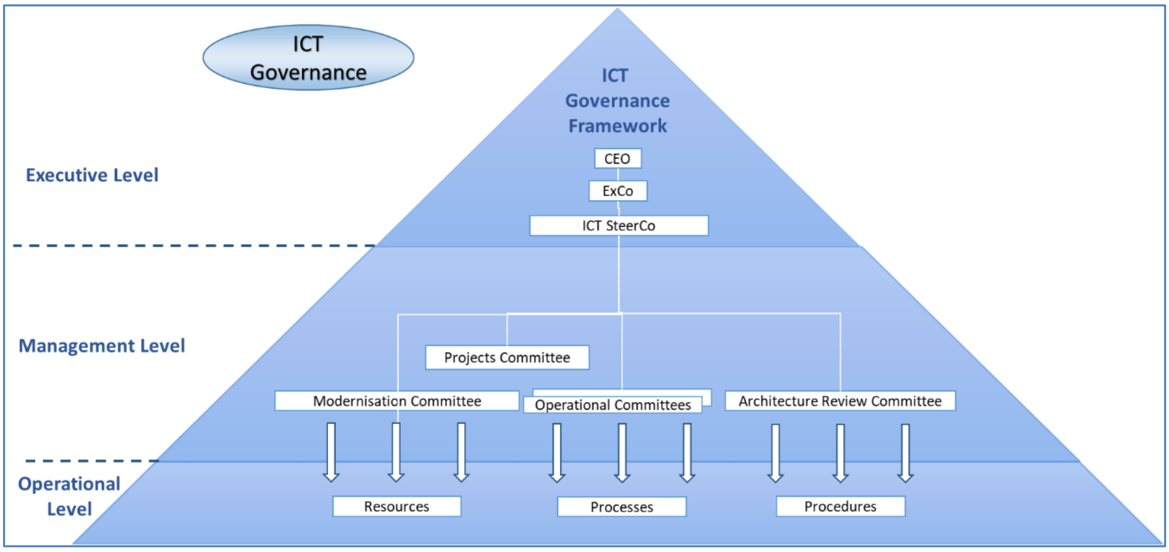


Figure 39 GPAA ICT Governance Structure

A high-level description of the committees who are in charge of ICT governance at GPAA follows:

Parties	Mandate
GPAA Executive Committee	• Setting the ICT Strategic direction.

	• It conceptualizes and oversees CGICT, GICT and strategic alignment. • coordinate and oversee the planning, implementation, and execution of the CGICT, GICT and strategic alignment and related monitoring activities.
ICT Steering Committee	• Provide leadership, direction and oversight for the design and implementation of the GPAA ICT strategy as determined by the GPAA Executive Committee.
Modernisation Committee	• Oversees and provides direction to significant GPAA initiatives that are intended provide significant improvements to the way that GPAA does its business in accordance with the ICT Strategic direction.
Architecture Review Committee	Evaluates and recommends architecture submissions for all Enterprise Architecture matters including Business, Applications, Data, Infrastructure architecture domains. Architecture recommendations are submitted to the ICT Steering committee for ratification.
Projects Committee	Enforcing the governance framework and ensure that ICT initiatives that are organised as projects are brought into successful completion within their determined budget and timelines, achieving their goals.
Operational Committees	• Tasked to ensure that ICT consistently and reliably supports the day-to-day activities of all processes at the GPAA that are enabled by ICT. Includes the following: • ICT Operational Committee, • Service Level Agreement (SLA) Committee, • Change Management Committee (CMC), • Triage Committee, • Service Continuity Committee and the ICT Information Security (IS) committee.

ICT Portfolio and Programme Management

The GPAA Programme/Project Management Framework defines the core processes for the Project Management Office (PMO). These represent the fundamental areas of responsibility that support

PMO activities. Application of strong project management principles and practices to these processes assists in building a long-term foundation and infrastructure for the PMO.

ICT Risk Management

The GPAA Enterprise Wide Risk Management (EWRM) Framework provides guidance to implement a consistent, efficient, and economical approach to identify, evaluate and respond to key risks that may impact business objectives. The Framework is based on the principles embodied in the Public Sector Risk Management Framework published by National Treasury, the Enterprise Risk Management Framework published by the Committee of Sponsoring Organisations (COSO) of the Treadway Commission, the King Code on Governance Principles **(King IV**), the Batho Pele principles, and ISO 31000.

Modernisation Programme Considerations

Current assessment of GPAA EA Practice

The EA Practice at GPAA is operates within the ICT Function and participates in the operational activities and implementation of technology initiatives and day-to-day operations.

The Practice is guided by the ICT Governance Framework for GPAA and represented as one of the committees, namely the Architecture Review Committee (ARC), thereby providing visibility within the organizational governance for ICT.

The team currently has a few members, but not sufficient to fulfil the requirements of an EA practice that covers the various domains across the various initiatives and organizational requirements.

The following suggestions are proposed for consideration for the Modernisation Programme.

- To engage resources that have competency in each of the EA following domains.
    - Enterprise Architecture
    - Business Architecture
    - Data Architecture
    - Applications Architecture
    - Cloud & Infrastructure Architecture
    - Security Architecture
- To create and update the EA Frameworks and Methodologies to adopt.

- To Model and document the GPAA Enterprise Architecture and overall environment. This requires acquisition of a suitable EA Modelling tool.
- To acquire a suitable EA Modelling tool. Archi can work as a temporary tool but would not be sufficient for more complex architecture modelling within each domain and does not provide many features compared to other tools.
- To provide a forum for Technical Solution Architecture reviews if the ARC does not deal with this. This forum would incorporate various technical personnel that are part of the various technology stacks, domains, products, and specialities, to collaborate and review solutions from a technical perspective.
- Creation of Technical Standards and Guidelines in the various domains
- Incorporation of EA consultation in Project initiation and Governance.

The following is the proposed understanding of the ARC.

Architecture Review Committee (ARC)

Participants:

- **Enterprise Architects:** Offer an overarching view on how changes impact the entire organization's architecture.
- **Solution Architects:** Share specifics on how a particular solution fits into the broader EA.
- **Domain Experts:** Provide knowledge on specific areas such as security, data, or applications.
- **IT Managers:** Give insights into feasibility, resource allocation, and technical standards.
- **Representatives from Business Units:** To ensure business needs and considerations are addressed.

Objectives:

- Review, evaluate, and approve or reject architectural decisions.
- Ensure alignment between proposed changes and the organization's architectural principles and guidelines.
- Monitor and manage technical debt and ensure architectural consistency.
- Provide a platform for discussing architectural challenges and opportunities.

A Architecture Principles

This appendix lists the principles in the basis of architecture at GPAA.

A.1 Business Architecture Principles

Table 3 list the principles used when determining the business at GPAA.

Table 3: Business Architecture Principles

	Principle Name	Statement	Rationale	Implications
1	Primacy of Principles	These principles of information management apply to all Organisations within the enterprise.	The only way we can provide a consistent and measurable level of quality information to decision-makers is if all Organisations abide by the principles.	• Without this principle, exclusions, favoritism, and inconsistency would rapidly undermine the management of information • Information management initiatives will not begin until they are examined for compliance with the principles • A conflict with a principle will be resolved by changing the framework of the initiative
2	Maximise Benefit to the Enterprise	Information management decisions are made to provide maximum benefit to the enterprise as a whole.	This principle embodies "service above self". Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular organizational perspective. Maximum return on investment requires information management decisions to adhere to enterprise-wide drivers and priorities. No minority group will detract from the benefit of the whole. However, this principle will not preclude any minority group from getting its job done.	• Achieving maximum enterprise-wide benefit will require changes in the way we plan and manage information - technology alone will not bring about this change • Some Organisations may have to concede their own preferences for the greater benefit of the entire enterprise • Application development priorities must be established by the entire enterprise for the entire enterprise • Applications components should be shared across organizational boundaries • Information management initiatives should be conducted in accordance with the enterprise plan • As needs arise, priorities must be adjusted; a forum with comprehensive enterprise representation should make these decisions

	Principle Name	Statement	Rationale	Implications
3	Information Management is Everybody's Business	All Organisations in the enterprise participate in information management decisions needed to accomplish business objectives.	Information users are the key stakeholders, or customers, in the application of technology to address a business need. In order to ensure information management is aligned with the business, all Organisations in the enterprise must be involved in all aspects of the information environment. The business experts from across the enterprise and the technical staff responsible for developing and sustaining the information environment need to come together as a team to jointly define the goals and objectives of IT.	• To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment • Commitment of resources will be required to implement this principle
4	Business Continuity	Enterprise operations are maintained in spite of system interruptions.	As system operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the enterprise must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop enterprise activities. The enterprise business functions must be capable of operating on alternative information delivery mechanisms.	• Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed • Recoverability, redundancy, and maintainability should be addressed at the time of design • Applications must be assessed for criticality and impact on the enterprise mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary

	Principle Name	Statement	Rationale	Implications
5	Common Use Applications	Development of applications used across the enterprise is preferred over the development of similar or duplicative applications which are only provided to a particular organization.	Duplicative capability is expensive and proliferates conflicting data.	• Organisations which depend on a capability which does not serve the entire enterprise must change over to the replacement enterprise-wide capability; this will require establishment of and adherence to a policy requiring this • Organisations will not be allowed to develop capabilities for their own use which are similar/duplicative of enterprise-wide capabilities; in this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced • Data and information used to support enterprise decision-making will be standardized to a much greater extent than previously
6	Service Orientation	The architecture is based on a design of services which mirror real-world business activities comprising the enterprise (or inter-enterprise) business processes.	Service orientation delivers enterprise agility and Boundaryless Information Flow.	• Service representation utilizes business descriptions to provide context (i.e., business process, goal, rule, policy, service interface, and service component) and implements services using service orchestration • Service orientation places unique requirements on the infrastructure, and implementations should use open standards to realize interoperability and location transparency • Implementations are environment-specific; they are constrained or enabled by context and must be described within that context • Strong governance of service representation and implementation is required • A "Litmus Test", which determines a "good service", is required
7	Compliance with Law	Enterprise information management processes comply with all relevant laws, policies, and regulations.	Enterprise policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations.	• The enterprise must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data • Education and access to the rules

	Principle Name	Statement	Rationale	Implications
8	IT Responsibility	The IT organization is responsible for owning and implementing IT processes and infrastructure that enable solutions to meet user-defined requirements for functionality, service levels, cost, and delivery timing.	Effectively align expectations with capabilities and costs so that all projects are cost-effective. Efficient and effective solutions have reasonable costs and clear benefits.	• A process must be created to prioritize projects • The IT function must define processes to manage business unit expectations • Data, application, and technology models must be created to enable integrated quality solutions and to maximize results
9	Protection of Intellectual Property	The enterprise's Intellectual Property (IP) must be protected. This protection must be reflected in the IT architecture, implementation, and governance processes.	A major part of an enterprise's IP is hosted in the IT domain.	• While protection of IP assets is everybody's business, much of the actual protection is implemented in the IT domain - even trust in non-IT processes can be managed by IT processes (email, mandatory notes, etc.) • A security policy, governing human and IT actors, will be required that can substantially improve protection of IP; this must be capable of both avoiding compromises and reducing liabilities • Balance protection of IP vs. transparency of information • Resources on such policies can be found at the SANS Institute

A.2 Data Architecture Principles

Table 4 provides a list of principles used when determining data architecture at the GPAA.

Table 4: Data Architecture Principles

	Principle Name	Statement	Rationale	Implications
10	Data is an Asset	Data is an asset that has value to the enterprise and is managed accordingly.	Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.	• This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible • Stewards must have the authority and means to manage the data for which they are accountable • We must make the cultural transition from "data ownership" thinking to "data stewardship" thinking • The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to enterprise personnel and adversely affect decisions across the enterprise • Part of the role of data steward, who manages the data, is to ensure data quality • A forum with comprehensive enterprise-wide representation should decide on process changes suggested by the steward • Since data is an asset of value to the entire enterprise, data stewards accountable for properly managing the data must be assigned at the enterprise level

11	Data is Shared	Users have access to the data necessary to perform their duties; therefore, data is shared across enterprise functions and organizations.	Timely access to accurate data is essential to improving the quality and efficiency of enterprise decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The enterprise holds a wealth of data, but it is stored in hundreds of incompatible stovepipe databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organization to efficiently share these islands of data across the organization. Shared data will result in improved decisions since we will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all of our decision-making. Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.	• This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible • To enable data sharing we must develop and abide by a common set of policies, procedures, and standards governing data management and access for both the short and the long term • For the short term, to preserve our significant investment in legacy systems, we must invest in software capable of migrating legacy system data into a shared data environment • We will also need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible • For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications • For both the short term and the long term we must adopt common methods and tools for creating, maintaining, and accessing the data shared across the enterprise • Data sharing will require a significant cultural change • This principle of data sharing will continually "bump up against" the principle of data security - under no circumstances will the data sharing principle cause confidential data to be compromised • Data made available for sharing will have to be relied upon by all users to execute their respective tasks

	Principle Name	Statement	Rationale	Implications
12	Data is Accessible	Data is accessible for users to perform their functions.	Wide access to data leads to efficiency and effectiveness in decision-making, and affords a timely response to information requests and service delivery. Using information must be considered from an enterprise perspective to allow access by a wide variety of users. Staff time is saved and consistency of data is improved.	• This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible • Accessibility involves the ease with which users obtain information • The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of enterprise users and their corresponding methods of access • Access to data does not constitute understanding of the data - personnel should take caution not to misinterpret information • Access to data does not necessarily grant the user access rights to modify or disclose the data
13	Data Trustee	Each data element has a trustee accountable for data quality.	One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the enterprise. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data trustee makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the data trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources. **Note:** A trustee is different than a steward - a trustee is responsible for accuracy and currency of the data, while responsibilities of a steward may be broader and include data standardization and definition tasks.	• Real trusteeship dissolves the data "ownership" issues and allows the data to be available to meet all users' needs • The data trustee will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable • It is essential that the trustee has the ability to provide user confidence in the data based upon attributes such as "data source" • It is essential to identify the true source of the data in order that the data authority can be assigned this trustee responsibility • Information should be captured electronically once and immediately validated as close to the source as possible • As a result of sharing data across the enterprise, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, subsequently, must then recognize the importance of this trusteeship responsibility

	Principle Name	Statement	Rationale	Implications
14	Common Vocabulary and Data Definitions	Data is defined consistently throughout the enterprise, and the definitions are understandable and available to all users.	The data that will be used in the development of applications must have a common definition throughout the Headquarters to enable sharing of data. A common vocabulary will facilitate communications and enable dialog to be effective. In addition, it is required to interface systems and exchange data.	• We are lulled into thinking that this issue is adequately addressed because there are people with "data administration" job titles and forums with charters implying responsibility • The enterprise must establish the initial common vocabulary for the business; the definitions will be used uniformly throughout the enterprise • Whenever a new data definition is required, the definition effort will be coordinated and reconciled with the corporate "glossary" of data descriptions • Ambiguities resulting from multiple parochial definitions of data must give way to accepted enterprise-wide definitions and understanding • Multiple data standardization initiatives need to be coordinated • Functional data administration responsibilities must be assigned

	Principle Name	Statement	Rationale	Implications
15	Data Security	Data is protected from unauthorized use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, sensitive, source selection-sensitive, and proprietary information.	Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information. Existing laws and regulations require the safeguarding of national security and the privacy of data, while permitting free and open access. Pre-decisional (work-in-progress, not yet authorized for release) information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.	• Aggregation of data, both classified and not, will create a large target requiring review and de-classification procedures to maintain appropriate control • The current practice of having separate systems to contain different classifications needs to be rethought • In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level • Data security safeguards can be put in place to restrict access to "view only" or "never see" • Security must be designed into data elements from the beginning; it cannot be added later • New policies are needed on managing duration of protection for pre-decisional information and other works-in-progress, in consideration of content freshness

A.3 Applications Architecture Principles

Table 5 lists the principles used to determine the application architecture at GPAA.

Table 5: Application Architecture Principles

	Principle Name	Statement	Rationale	Implications
16	Technology Independence	Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.	Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way. Otherwise technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves. Realizing that every decision made with respect to IT makes us dependent on that technology, the intent of this principle is to ensure that Application Software is not dependent on specific hardware and operating systems software.	• This principle will require standards which support portability • For Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) applications, there may be limited current choices, as many of these applications are technology and platform-dependent • Subsystem interfaces will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the Enterprise Architecture • Middleware should be used to decouple applications from specific software solutions • As an example, this principle could lead to use of Java, and future Java-like protocols, which give a high degree of priority to platform-independence

	Principle Name	Statement	Rationale	Implications
17	Ease-of-Use	Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand.	The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for use of applications. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task outside of the enterprise's integrated information environment. Most of the knowledge required to operate one system will be similar to others. Training is kept to a minimum, and the risk of using a system improperly is low. Using an application should be as intuitive as driving a different car.	• Applications will be required to have a common "look-and-feel" and support ergonomic requirements; hence, the common look-and-feel standard must be designed and usability test criteria must be developed • Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability • Ease of use and intuitive use of applications must be designed into the applications from the start. Not just having the required functionality.

A.4 Technology Architecture Principles

Table 6 lists the principles used to determine the PAA technology architecture.

Table 6: Technology Architecture Principles

	Principle Name	Statement	Rationale	Implications
18	Requirements-Based Change	Only in response to business needs are changes to applications and technology made.	This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to IT changes. This is to ensure that the purpose of the information support - the transaction of business - is the basis for any proposed change. Unintended effects on business due to IT changes will be minimized. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.	• Changes in implementation will follow full examination of the proposed changes using the Enterprise Architecture • There is no funding for a technical improvement or system development unless a documented business need exists • Change management processes conforming to this principle will be developed and implemented • This principle may bump up against the responsive change principle
19	Responsive Change Management	Changes to the enterprise information environment are implemented in a timely manner.	If people are to be expected to work within the enterprise information environment, that information environment must be responsive to their needs.	• Processes for managing and implementing change must be developed that do not create delays • A user who feels a need for change will need to connect with a "business expert" to facilitate explanation and implementation of that need • If changes are going to be made, the architectures must be kept updated • Adopting this principle might require additional resources • This will conflict with other principles (e.g., maximum enterprise-wide benefit, enterprise-wide applications, etc.)

	Principle Name	Statement	Rationale	Implications
20	Control Technical Diversity	Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.	There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained. Limiting the number of supported components will simplify maintainability and reduce costs. The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the enterprise brings the benefits of economies of scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.	• Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle • Technology choices will be constrained by the choices available within the technology blueprint • The technology baseline is not being frozen
21	Interoperability	Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.	Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products and facilitate supply chain integration.	• Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution • A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established • The existing IT platforms must be identified and documented

B Information Model Definitions and Relationships

Table 7: Information Map Definitions

Information Concepts	Definition
Beneficiary	A person who has received or is still receiving the benefits after application of the product rules. A beneficiary can be one or more of the following: Pensioner Spouse pensioner Child pensioner Orphan Special pensioner Funeral Benefit recipient Military Medical beneficiary Special pensioner
Benefit	The actual monetary value that a beneficiary is entitled to as a result of applied product rules. A benefit can be one or more of the following: Resignation or Retirement Benefit Funeral Benefit Spouse Benefit Orphan Benefit Child Benefit Military Medical Benefits Medical Subsidy Additional Voluntary Contributions Clean Break
Case	A formal request triggered by a client executed by a predefined set of actions sequenced and tracked with the purpose of fulfilling a formal request within a predetermined time frame

Information Concepts	Definition
Channel	A communication route for communication from and to our clients, members and beneficiaries. Channels are one or more of the following: Telephone Email SMS Fax Self Service Call Centre Walk-in Centre
Client	Any entity who interacts with the Administrator in his own capacity or on behalf of another person. A client can be one or more of the following: Member Beneficiary Employer Relative of friend of a member or beneficiary Broker
Contribution	A payment for the purpose of building a fund for a specific purpose
Customer	An organisation on whose behalf the Administrator (GPAA) administers its benefits GPAA customers are the following; Government Employees Pension Fund (GEPF) National Treasury (NT)
Debt	A sum of money that is owed because of the various debt payment arrangements between a member, employer and the GPAA. Examples of debt are: Employer debt Member debt
Employer	An organisation that employs the member and usually is responsible for paying the contribution

Information Concepts	Definition
Evidence	Tagged images or structured data representations submitted to the Administrator as proof to validate the information. Examples of evidence are: Copy of ID Employment record Death certificate Marriage certificate
Key Partner	Organisations that the Administrator is dependent on so that services are delivered effectively and efficiently. GPAA main key partners are, but can change over time: SafetyWeb Verification of injury partners for Military Medical SARS
Member	A person who has been admitted to a fund and is entitled to benefits as described in the product rules
Organisation	An organized group of people within GPAA with a particular purpose. Examples are the sections within GPAA, but could also be a project team, committee or council.
Operational Finance	The management of money flowing into and out of bank accounts.
Payment	The actual benefit of a recipient that is paid into a specific bank account
Payment Channel	A payment route to enable payment to our beneficiaries
Product	A set of rules that define the eligibility (conditions of receipt) of an individual and potential benefit(s) (calculation formula) that a product must provide to this individual in the occurrence of life events as described in said rules. Benefits are: Pension Benefits Medical Subsidies Injury on Duty (IOD) Military Medical Special Pension VIP (Parliamentary members)

Table 8: Information Map Relationships

Relationship	Business Rule
Customer - Product	Product rules can only be supplied by the Customer
Product - Member	Conditions for a member's membership can only be determined by the Product Rules
Product - Contribution	The contribution amount can only be determined by the Product Rules
Member - Contribution	A member must contribute to the Fund
Product - Client	The product rules determine whether a client is entitled to benefits
Product - Benefit	The Benefit can only be determined by the product rules
Channel - Case	A case can only be registered if received via a channel
Channel - Evidence	Evidence can only be received via a channel
Case - Evidence	A case can only be processed if required evidence is supplied
Case - Key Partner	Key partners enable the case resolution process
Case - Benefit	A benefit can only be made available after processing of a case
Benefit - Beneficiary	A benefit must be paid to a beneficiary
Beneficiary - Key Partner	Beneficiary life verification must be done via a key partner
Member - Employer	A member works for the employer
Employer - Contribution	The employer must pay both the member and the employer contribution
Employer - Debt	The employer must pay member debt related to contributions
Debt - Contribution	A debt must be created for an arrear contribution
Payment - Payment Channel	A payment must be made through a recognised payment channel
Beneficiary - Payment channel	Every beneficiary must have a payment channel
Member - Key Partner	Member information must be confirmed via a key partner
Organisation - Case	An organisation must work on a case

C Application Inventory and Future Plans

Table 9 provides a list of applications in production at the GPAA, their description, pain points and future plans for these applications. These applications are used by GPAA to carry out its mandate.

Table 9: Operational Applications Inventory

System	Description	Issues & Pain Points	Future Plans
ACL	Audit		
AD Manager	Active Directory for access to systems		Retain
Adastrip	Data Extracts on CIVPEN	Mainframe application.	Discontinue once the Mainframe is replaced.
Adobe Acrobat Reader	PDF reader		Retain
BarnOwl	Audit & Risk tool		
BARR Printing	Mainframe Printing	Part of the Mainframe architecture	Discontinue once the Mainframe is replaced and document printing is moved off the Mainframe.
Bateleur E-Strip	Data extraction from CIVPEN database	Part of the Mainframe technology	Decommission when the Mainframe is replaced
Bespoke Java/JavaScript Applications	Fund administration services and business processes		Retain and implement as micro-services
BPA/PCM	Exit Claim Management including submission of exit claims from the employers and benefit payment processing	Monolith. Automated finalisation of exit claims is lower than expected	Retain and develop

System	Description	Issues & Pain Points	Future Plans
CIC	Outsourced telephony integration and front end application for Call Centre agents	No integration with GPAA's back end services and applications	Provide a Client Relationship Management that includes multi-channel integration and integration with GPAA back-end services
Cisco Call Attendant	Call Attendant software	Duplication with CIC	Decommission and replace with the CRM application or with modern communication facilities (MS Teams, WebEx)
Cisco Call Manager (UC)	Unified Communication (phones)	Aging technology	Replace with modern communication facilities (MS Teams, WebEx)
CITRIX	Thin Client application	Used as a platform for a small and diminishing set of applications. Current implementation is outdated.	Decommission or expand into full implementation of thin client implementation at GPAA
CIVPEN	Main Pension Administration System for the GPAA	Aging technology and application	Replace with bespoke, procured or a combination of both.
Computer Associates (Mainframe Software)	Computer Associates software licenses for the mainframe	Part of the Mainframe architecture	Replace when the Mainframe is replaced and decommissioned

System	Description	Issues & Pain Points	Future Plans
Computer Associates (XCOM Encryption)	Secure, encrypted and managed file exchange for Bankserv files	Duplicate technology with Connect:Direct. Implemented using old technology (VB ver. 6)	Replace with a Java service and Connect:Direct. Decommission XCOM.
Connect:Direct	Secure file exchange with 3rd parties		Retain and expand
Digital Communication Platform	Provide a platform for large scale communication capability (via email and SMS) to members and pensioners and any other target population. Intended to replace printed document mailing.		Retain and expand
EDMS	Enterprise Data Management System Data Quality Management Infomet	Rules engine and intellectual properties does not belong to GPAA	Decommission
E-Workflow (BPM)	Workflow software	Duplication with Oracle BPM	Decommission and replace with Oracle BPM
Self-Service Portal	Member/Pensioner Self-Service Portal	Incomplete implementation	Retain and Expand

System	Description	Issues & Pain Points	Future Plans
Mobile App	Provides access to the same capabilities as provided in the self-service portal, but through a mobile application	Incomplete implementation	Retain and Expand
LawTrust Digital Signatures	Digital signatures on electronic documents		Retain
LIBWIN	Library management software	.Net based. No integration with any other applications and components at GPAA	Consider replacement
McAfee ePO	Anti-virus and end point data protection software		To be replaced
Microsoft	Microsoft software products: Document editor, spreadsheet editor, presentation editor, diagram editor, project management utility		Retain
Mindjet MindManager	Mind Mapping tool		Retain
MS Outlook and Exchange	Mail System – Server and Front-End		Retain
ODS	Tax Directive System	Aging application, monolith. Some integration with current GPAA applications	Rewrite
Oracle BI Enterprise Edition	Business Intelligence and reporting solution		Retain and expand

System	Description	Issues & Pain Points	Future Plans
Oracle BPM	Business Process management software		Retain and expand
Oracle Database	Database software		Retain
Oracle IAM	Identity and Access management		Retain and expand
Oracle old Portal applications	General Enquiries, Cashbook, Bank Reconciliation, MLV, etc.	Old technology. Replacement urgently required	Replace with either purchased components or bespoke developed components
Oracle Service Bus	An integration infrastructure providing interaction capabilities between services and applications	Implementation efforts are still required	Retain. Evaluate role in light of the emergence of Micro-services architecture.
Oracle SOA Suite	A suite of utility that enables the use implementation of business processes within GPAA	Implementation efforts are still required	Retain. Evaluate role in light of the emergence of Micro-services architecture.
Pekwa	Legacy Content Management System.	Old technology (implemented using MS VB 6), Partial capability for handling PDF documents. Requires urgent replacement	Replace with Oracle WebCenter Content and Oracle WebCenter Capture.
PEKWA (Other Applications)	Various other Legacy applications implemented on Pekwa	Old technology (implemented using MS VB 6)	Evaluate all applications on Pekwa for replacement alternatives

System	Description	Issues & Pain Points	Future Plans
Pervasent Boardpapers	Document packaging and distribution for board and committee documents.		To be decommissioned.
PhoneX	Phone Manager	Very little integration	Consider replacement
Queue Management System Emerge/Qmatic	WIC Queue management system		Retain
Sage ERP 300 (ACCPAC)	ERP	Integration with CIVPEN only.	Replace with off the shelf components that can be easily integrated with the Oracle Fusion stack.
SharePoint (GEPF)	SharePoint Web site, Intranet, team sites.	User acceptance	Retain and expand
SharePoint (GPAA)	SharePoint Web site, Intranet, team sites.	User acceptance	Retain and expand
SharePoint Project Server (GPAA)	Project services	Availability of implementation skills	Implement
Software AG - Natural, Adabas	Mainframe database and software development language used for developing and maintain CIVPEN	Used for CIVPEN application that is planned for replacement	Maintain until CIVPEN replacement
Solimar Printing Images/Mainframe	Mainframe formatted printing	Part of the Mainframe architecture	Maintain until Mainframe printing is discontinued
TeamMate	Audit & Risk		

System	Description	Issues & Pain Points	Future Plans
TotemoData	Data encryption	Duplicate functionality with Connect:Direct and XCOM	Decommission
TotemoMail	Secure, encrypted mail delivery	Implementation was completed but not utilised.	Decommission
Vendor Relationship Management (VRM)	Vendor Relationship Management		
WebCenter Content	Electronic Content Management	Transition between Pekwa and WebCenter Content	Use as the GPAA Enterprise Content Management repository

Table 10 provides a list of applications that are used by GPAA as part of its software development life cycle to install, develop and configure applications for GPAA operational use.

Table 10: Development Applications Inventory

System	Description	Issues & Pain Points	Future Plans
Adobe Acrobat Reader	PDF reader		Retain
Bitbucket	Source code repository utility supporting Software Development Life Cycle		Retain
Confluence	Application documentation portal used during Software Development Life Cycle	Functional duplication with MS SharePoint	Retain

System	Description	Issues & Pain Points	Future Plans
Crowd	Access control for Jira, Confluence used for Software Development Life Cycle. Integrates with MS Active Directory.		Retain. Evaluate the role of Crowd vs the role of Oracle IAM.
Intellij IDEA	An Integrated Development Environment for developing Java and JavaScript Based applications		Retain and use in conjunction with Oracle jDeveloper
Jira	Issue Management application used during the Software Development Life Cycle		Retain
Microsoft Productivity Suite	Microsoft software products: Document editor, spreadsheet editor, presentation editor, diagram editor, project management utility		Retain
Microsoft SharePoint	SharePoint Web site, Intranet, team sites.	Availability of skills	Retain and expand
MS Outlook and Exchange	Mail System – Server and Front-End		Retain
Oracle BI	Business Intelligence and reporting solution		Retain and expand
Oracle BPM	Business Process management software		Retain and expand
Oracle Database	Database software		Retain
Oracle IAM	Identity and Access management	Implementation effort is still required	Retain and expand
Oracle jDeveloper	An Integrated Development Environment for developing Java and Oracle based applications	Small market share. Not widely known by Java developers	Retain and use in conjunction with Intellij IDEA

System	Description	Issues & Pain Points	Future Plans
Oracle Service Bus (OSB)	An integration infrastructure providing interaction capabilities between services and applications	Implementation efforts are still required	Retain. Evaluate role in light of the emergence of Micro-services architecture.
Oracle SOA Suite	A suite of utility that enables the use implementation of business processes within GPAA	Implementation efforts are still required	Retain. Evaluate role in light of the emergence of Micro-services architecture.
Oracle SQL Developer	A database access and development tool, mainly for Oracle databases		Retain
Oracle WebCenter Content and WebCenter Capture	Electronic Content Management	Transition between Pekwa and WebCenter Content	Use as the GPAA Enterprise Content Management repository
REMAS	A bespoke developed application for logging and tracking issues for the CIVPEN application.	Implemented on an unsupported technology.	Migrate functionality to Jira.
Software AG - ARIS	Business Process Business Analysis and model repository tool	Limited skills of ARIS administration	Retain and expand
Software AG - Natural, Adabas	Mainframe database and software development language used for developing and maintain CIVPEN	Aged technology with limited capabilities. Availability of skills is declining	Maintain until CIVPEN replacement. Move to NaturalOne.

Table 11 provides a list of applications and facilities that are being used to monitor the health of the operational ICT environment of GPAA, identify any emerging issues and enable quick corrective action to prevent deterioration and outage in any of the components of the GPAA operational environment. These applications and facilities are critical in maintaining high availability of the GPAA operational environment.

Table 11: Environment Monitoring Utilities Inventory

System	Description	Issues & Pain Points	Future Plans
Checkmk	IT Infrastructure Monitoring facility that is working in conjunction with Nagios		Retain and expand
Cisco Prime	Cisco Monitoring Tool. Enable central and controlled upgrade of network devices.		Integrate monitoring data into consolidated GPAA monitoring facilities
Nagios	IT Infrastructure Monitoring facility that is working in conjunction with Checkmk		Retain and expand
Oracle BAM	Used for monitoring the health of business processes within the GPAA environment	Implementation efforts are still outstanding	Retain and expand
Oracle BI	Business Intelligence and reporting solution that is also used for monitoring the health of the IT Infrastructure		Retain and expand