Data & Information Protection - Target state Modernisation roadmap

Author	Francis Kaitano, Glenn Ballam, Hugh Walcott, John Marshall, Tracey Davis
Date Produced & Version	August 2025 v0.2
Responsible Head of Architecture	Tanya Boelema, Angus Cotton
Enterprise Owners	Richard Boxall, Chief Information Security Officer Kate Skinner, Executive – Digital, Data & Analytics Paul Norman, Executive – Chief Information Officer

Table of Contents

Executive Summary

Data & Information Protection

The strategy, process, technology and practice for safe, reliable, trusted and compliant data and information.

The target state enables BNZ to move faster, operate safer and lead with confidence in a digital first, regulated world.

Re-use the capabilities in existing technologies across platforms to uplift Data & Information Protection capability across the enterprise

Define and communicate **standards, patterns & tools** for the enterprise to ensure consistent protection practices and streamline compliance

Apply **DataSecOps** to embed automated Data & Information protection continuously across the lifecycle to ensure protection is built-in rather than added as an afterthought.

Introduce Data & Information Protection **Observability** across the enterprise to gain real-time visibility into sensitive data usage, threat detection and compliance

Introduce **Automation** in detection & response, to rapidly identify and mitigate threats while reducing manual effort and response time.

Look for **efficiency gains in AI** that can improve Data & Information Protection

Scope & Context

Effective Data & Information Protection requires deep integration with where data lives and moves – across the entire technology ecosystem, not within the boundaries of any single platform.

Transformation Approach

An evolution from reactive, siloed cybersecurity practices to a unified model that embeds governance, security, and technology across platforms and teams. Using a technology enabled phase as a bridge, to build the operational maturity needed to achieve enterprise-wide trust, resilience and agility.

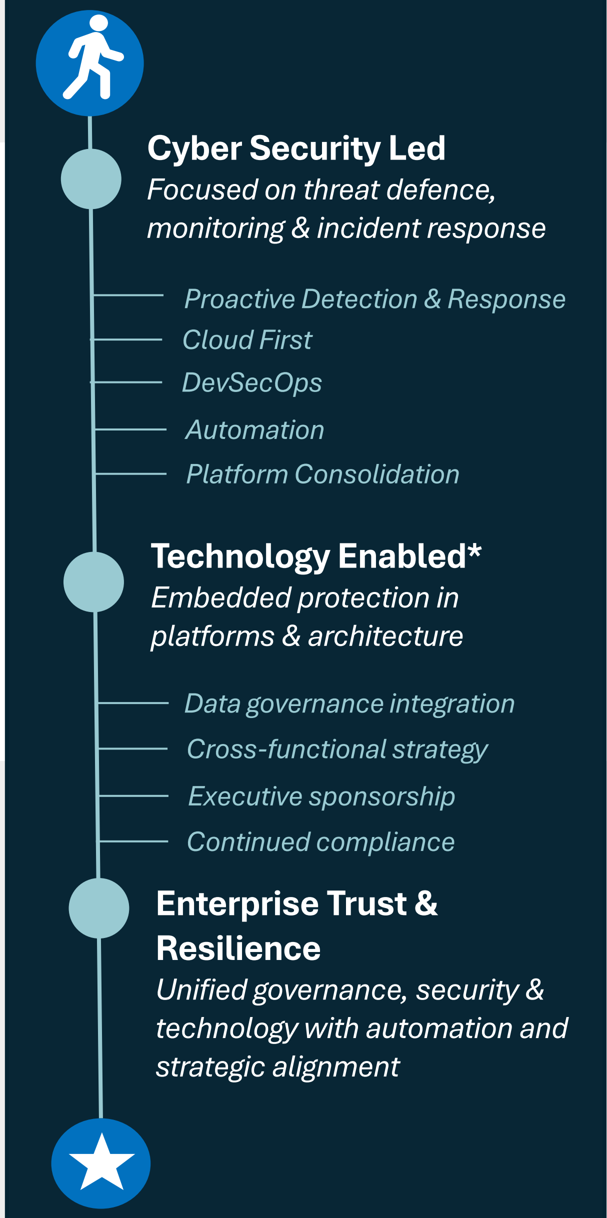
Current State - BMI View

BMI is represented in technologies across other platforms in BNZ, rather than in Data & Information Protection itself.

NAB Alignment

NAB haven't adopted Data & Information Protection as a platform, however the approach is similar in building protection with capabilities from other platforms. BNZ & NAB are targeting similar outcomes across contributing platforms e.g. secure-by-design, proactive risk and threat informed protection.

Modernisation Roadmap



Cyber Security Led

Focused on threat defence, monitoring & incident response

- *Proactive Detection & Response*
- *Cloud First*
- *DevSecOps*
- *Automation*
- *Platform Consolidation*

Technology Enabled*

Embedded protection in platforms & architecture

- *Data governance integration*
- *Cross-functional strategy*
- *Executive sponsorship*
- *Continued compliance*

Enterprise Trust & Resilience

Unified governance, security & technology with automation and strategic alignment

** Technology Enabled - some work in this phase already*

Data & Information Protection

Challenges & Issues

Fragmented Foundations & Inconsistent Practices Legacy tools and siloed operations have led to inconsistent policy enforcement, missing Zero Trust capabilities, and low data protection maturity across the enterprise.

Governance & Visibility
Fragmented tooling and lack of integration limit end-to-end observability, while gaps in unstructured data protection, retention, and access controls undermine governance and assurance across the data lifecycle.

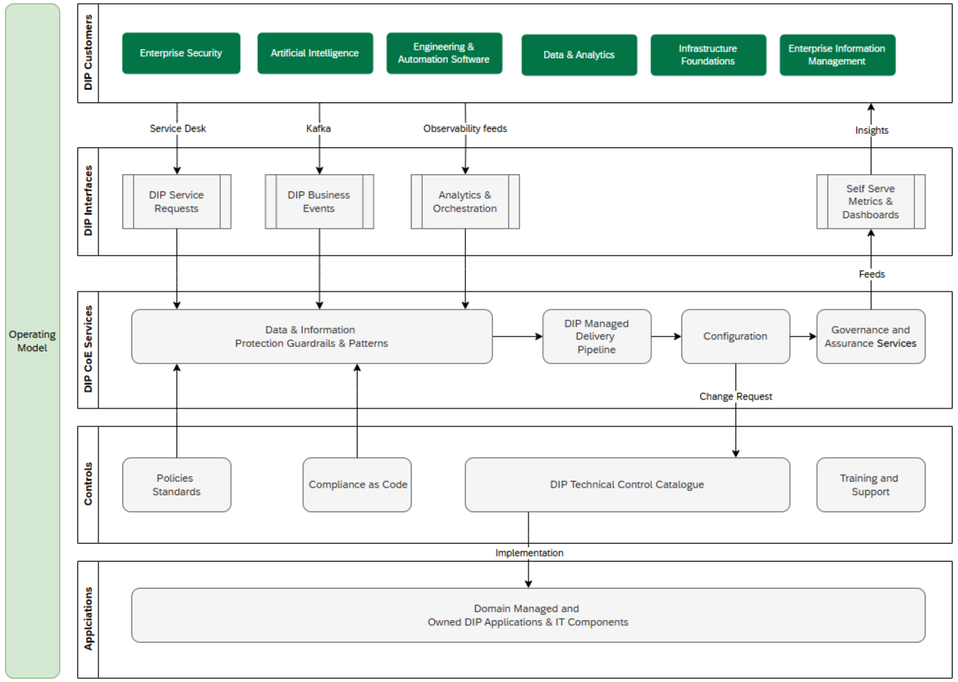
Operating Model & Capability Maturity
The organisation lacks a fit-for-purpose model and sufficient capability depth, with fragmented risk ownership, constrained investment, and limited commitment to uplift.

Culture & Communication
Data & Information Protection uplift is seen as a productivity barrier, with limited business-led dialogue, unclear stewardship roles, and a need for broader communication to build confidence.

Key Points

- **Interface Layer** Defining how to engage platform support and delivery services.
- **CoE Services Layer** Provides a platform service catalogue for the delivery of configuration changes, recommendations and insights
- **DIP Control Layer** Catalogue of governed risk mitigations, including policies, standards, training and support
- **Application Support Layer** representing the technologies responsible for implementing the configuration changes.

Target State Overview


Operating Model
DIP Customers
Enterprise Security
Artificial Intelligence
Engineering & Automation Software
Data & Analytics
Infrastructure Foundations
Enterprise Information Management
Service Desk
Kafka
Observability feeds
Insights
DIP Interfaces
DIP Service Requests
DIP Business Events
Analytics & Orchestration
Self Serve Metrics & Dashboards
Feeds
DIP CoE Services
Data & Information Protection Guardrails & Patterns
DIP Managed Delivery Pipeline
Configuration
Governance and Assurance Services
Change Request
Controls
Policies Standards
Compliance as Code
DIP Technical Control Catalogue
Training and Support
Implementation
Applciations
Domain Managed and Owned DIP Applications & IT Components

Technical Focus Areas

Uplift

- **Zero Trust Architecture –** shift from implicit trust to verify every access.
- **Event-driven & Decoupled Systems Security –** strengthening system resilience by securing data, detecting anomalies, and ensuring accuracy amongst platforms.
- **Synthetic Data & Data Simulation –** for testing and training (AI).
- **Data Detection & Response Uplift –** proactive detection and response to threats and breaches.
- **Data Security Posture & Configuration -** automation of capabilities responsible for identifying exposures and misconfiguration across our data assets, and their mitigations.
- **Channel Loss Prevention Uplift -** strengthening breadth and coverage across channels.

Future focussed

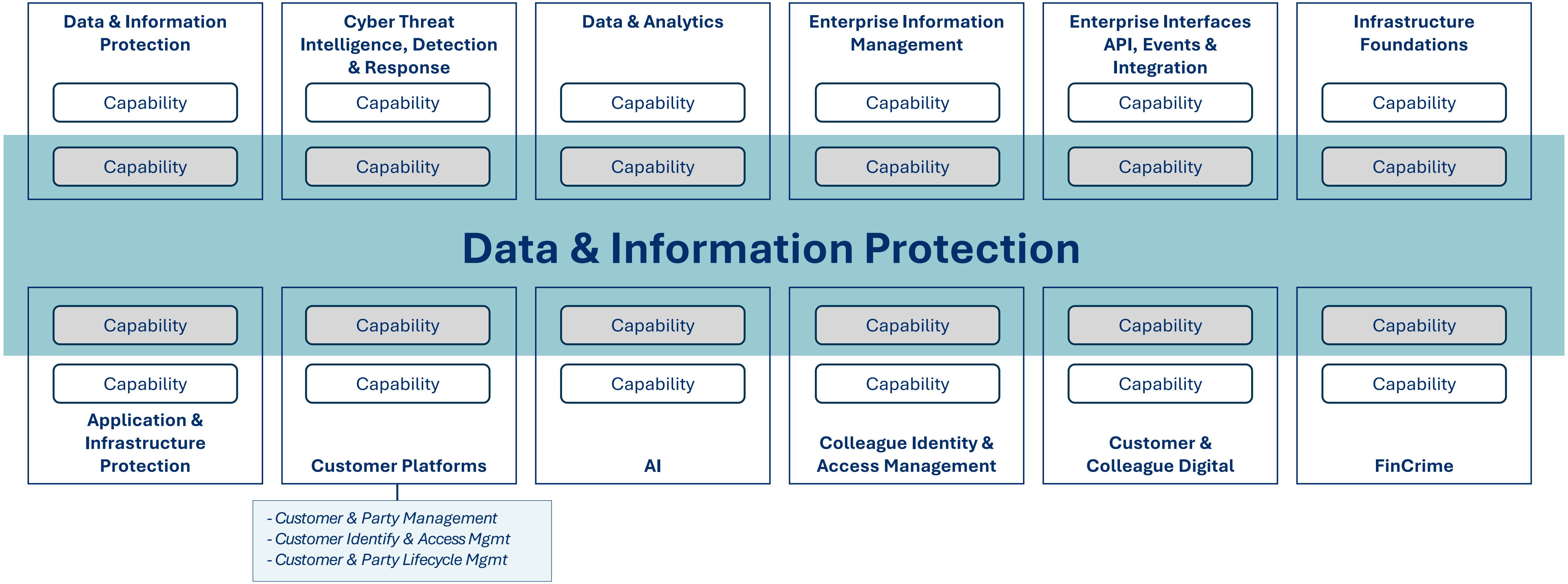
- **AI Readiness –** prepare to safely and effectively adopt and scale AI technologies.
- **Privacy-enhancing technologies –** trusted execution environments to protect sensitive data and code during processing.
- **Post Quantum cryptography –** vulnerability for traditional encryption methods as quantum computing advances.
- **AI Opportunities –** understand how AI can enhance Data & Information protection.
- **Data Sovereignty & cross border compliance –** Enable geo-fencing, data residency, and jurisdiction-aware handling.
- **Resilience against ransomware & data tampering –** confidential computing, immutable storage, air-gapped recovery, tamper-proof logs.

1. Platform Scope

Definition & Platform Context

Data & Information Protection is the strategy, process, technology and practice for safe, reliable, trusted and compliant data and information.

Effective Data & Information Protection requires deep integration with where data lives and moves – across the entire technology ecosystem, **not within the boundaries of any single platform**.



Data & Information Protection

Capability

Capability

Cyber Threat Intelligence, Detection & Response

Capability

Capability

Data & Analytics

Capability

Capability

Enterprise Information Management

Capability

Capability

Enterprise Interfaces API, Events & Integration

Capability

Capability

Infrastructure Foundations

Capability

Capability

Data & Information Protection

Capability

Capability

Application & Infrastructure Protection

Capability

Capability

Customer Platforms

- Customer & Party Management
- Customer Identify & Access Mgmt
- Customer & Party Lifecycle Mgmt

Capability

Capability

AI

Capability

Capability

Colleague Identity & Access Management

Capability

Capability

Customer & Colleague Digital

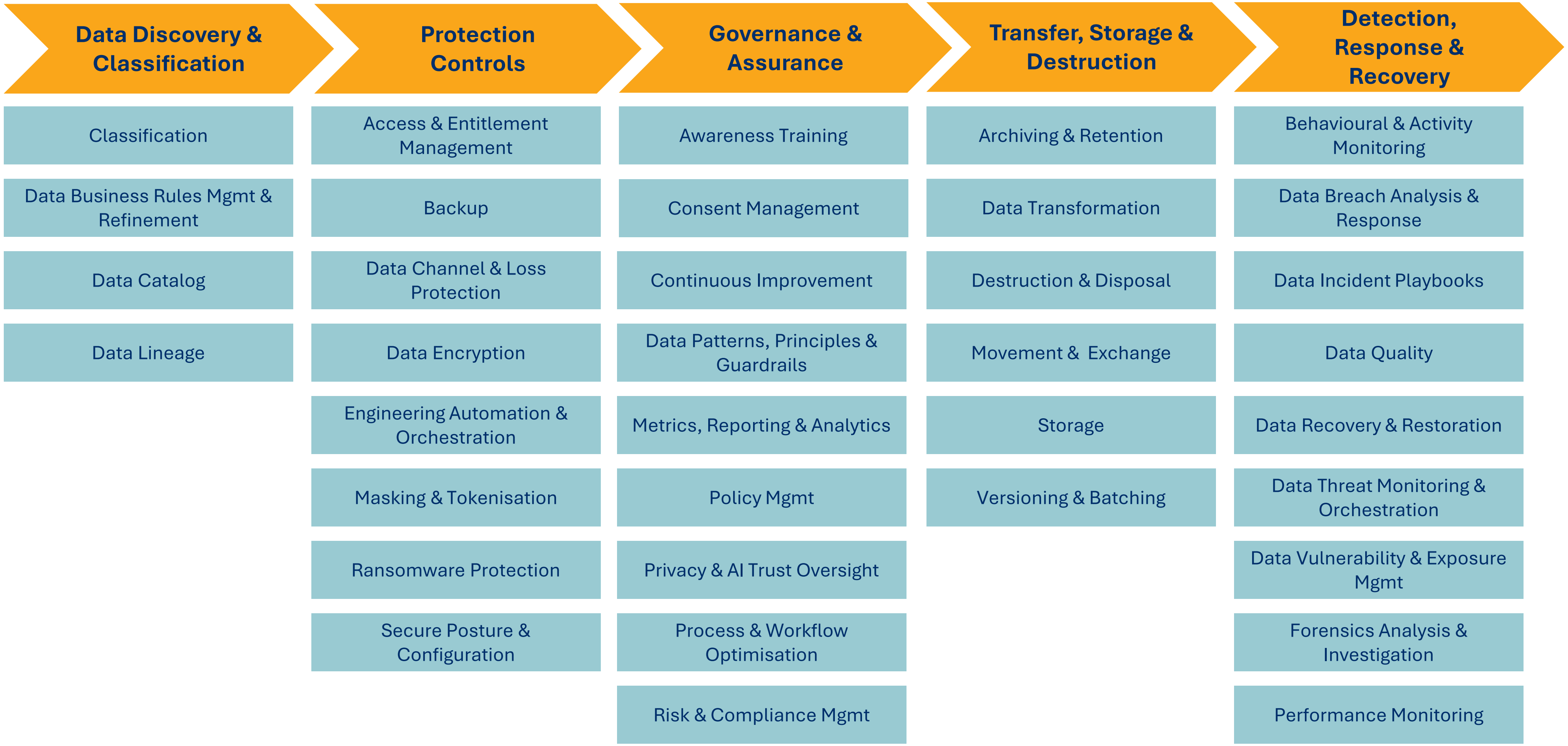
Capability

Capability

FinCrime

Value Chain & Capabilities

The value chain describes the activity and capabilities that allow us to achieve Data & Information Protection at BNZ



Data Discovery & Classification	Protection Controls	Governance & Assurance	Transfer, Storage & Destruction	Detection, Response & Recovery
Classification	Access & Entitlement Management	Awareness Training	Archiving & Retention	Behavioural & Activity Monitoring
Data Business Rules Mgmt & Refinement	Backup	Consent Management	Data Transformation	Data Breach Analysis & Response
Data Catalog	Data Channel & Loss Protection	Continuous Improvement	Destruction & Disposal	Data Incident Playbooks
Data Lineage	Data Encryption	Data Patterns, Principles & Guardrails	Movement & Exchange	Data Quality
	Engineering Automation & Orchestration	Metrics, Reporting & Analytics	Storage	Data Recovery & Restoration
	Masking & Tokenisation	Policy Mgmt	Versioning & Batching	Data Threat Monitoring & Orchestration
	Ransomware Protection	Privacy & AI Trust Oversight		Data Vulnerability & Exposure Mgmt
	Secure Posture & Configuration	Process & Workflow Optimisation		Forensics Analysis & Investigation
		Risk & Compliance Mgmt		Performance Monitoring

Note: *Value chain & capability definition in the appendix.*

Data & Information Protection Platform Context

The strategy, process and technology for **safe**, **reliable**, **trusted** and **compliant** data and information.

- Customer confidence & trust
- Business continuity & resilience
- Compliance & regulator expectations

Strategic Drivers

the 'why'

- Customers
- Colleagues
- Party – Prospects, Partners, Regulators, Vendors etc

Personas

the 'who'

- Regulations
- Risk Management
- Policies & Standards
- Controls

Governance

the 'what'

- Access Enablement
- Protection
- Detection & Response
- Operational resilience

Security

the 'how'

All data types

Across the whole lifecycle

Everywhere data & information lives and moves

Continuously

Through automation & orchestration

Data & Information Protection Break Down

Data Types

All data formats including structured data, unstructured data across operational and analytical systems and processes.

Data Lifecycle

Protection across the data lifecycle – Capture, Process, Retain, Distribute, Dispose.

Security Coverage

Protection of data in use, during transmission (in transit) and while stored (at rest), across all environments.

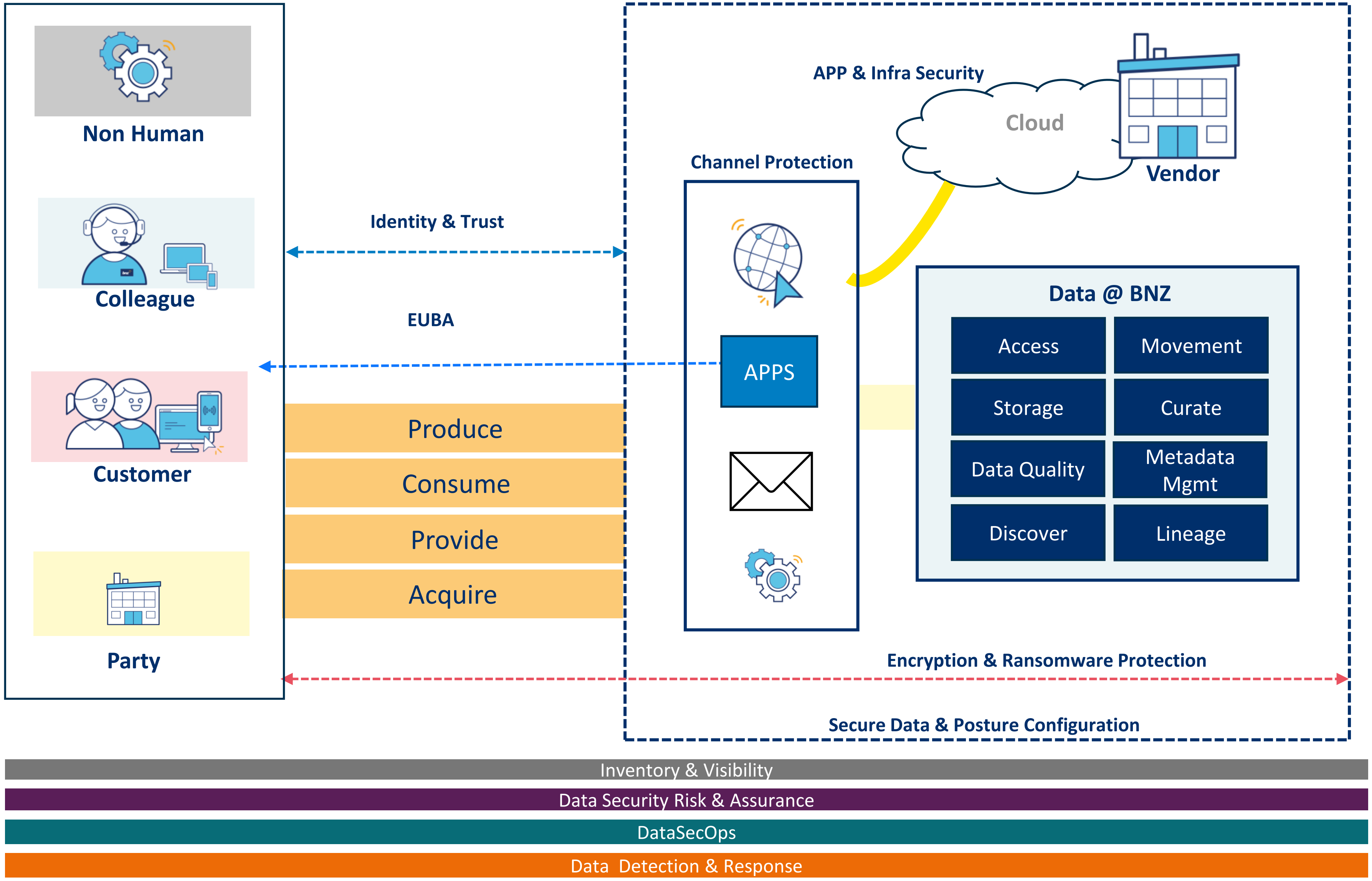
Risk Informed

Embedded, automated controls to deliver continuous security, assurance to meet compliance obligations and standards.

Resilient Access

Ensuring **appropriate** availability & access to data and information as and when it is required, without compromising its integrity.

Security Perspective (The How)



1. **Non Human** - AI, APIs, Microservices, system-system, cloud endpoint APIs, etc.

2. **Party -** Prospects, Partners, Regulatory bodies, vendors, etc

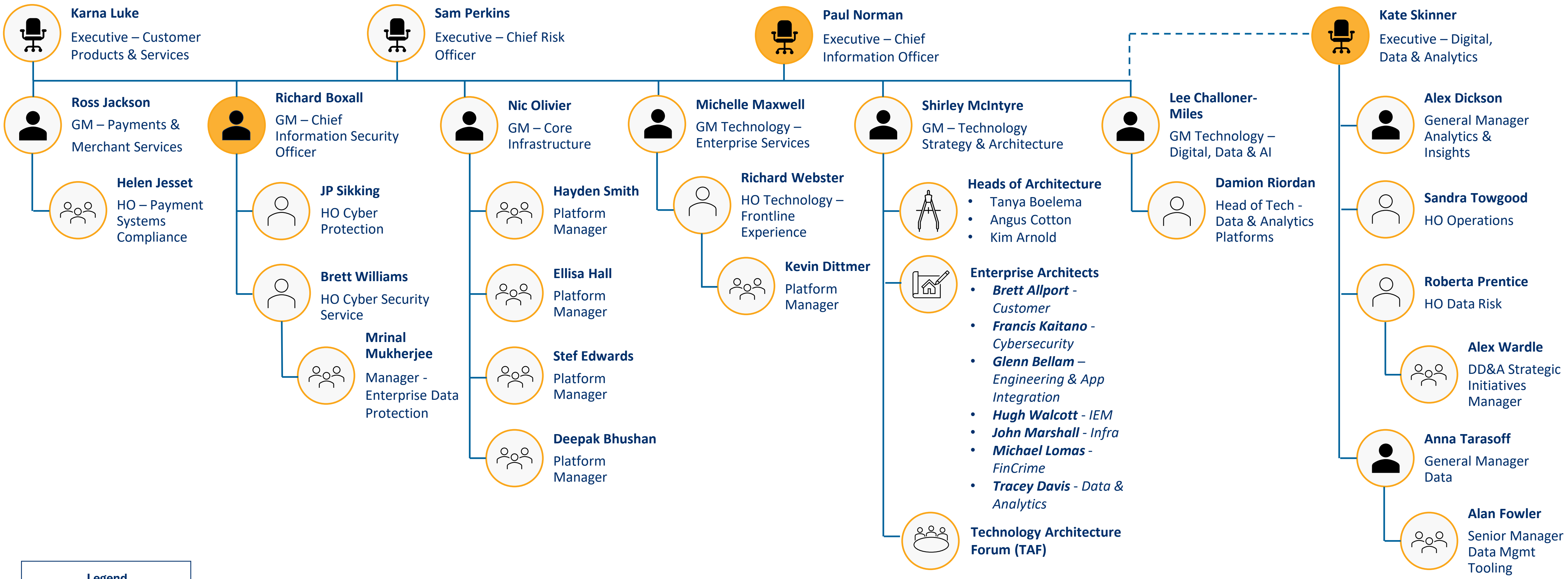
3. **Identity & Trust** covers human, non human entities including secret management, privilege access.

4. **DataSecOps** include Automation of security controls across the DataOps and managed pipelines.

5. Inventory, Visibility, risk, assurance , Detection and Response are continuous and flow through across the journey touchpoints.

6. **User, Entity Behavioural Analytics(EUBA**)covers the insider risk and threats associated with entity and user behavioural aspects for use of data including database activity monitoring.

Stakeholder Engagement & Accountability



Karna Luke
Executive – Customer Products & Services

Sam Perkins
Executive – Chief Risk Officer

Paul Norman
Executive – Chief Information Officer

Kate Skinner
Executive – Digital, Data & Analytics

Ross Jackson
GM – Payments & Merchant Services

Helen Jesset
HO – Payment Systems Compliance

Richard Boxall
GM – Chief Information Security Officer

JP Sikking
HO Cyber Protection

Brett Williams
HO Cyber Security Service

Mrinal Mukherjee
Manager - Enterprise Data Protection

Nic Olivier
GM – Core Infrastructure

Hayden Smith
Platform Manager

Ellisa Hall
Platform Manager

Stef Edwards
Platform Manager

Deepak Bhushan
Platform Manager

Michelle Maxwell
GM Technology – Enterprise Services

Richard Webster
HO Technology – Frontline Experience

Kevin Dittmer
Platform Manager

Shirley McIntyre
GM – Technology Strategy & Architecture

Heads of Architecture
- Tanya Boelema
- Angus Cotton
- Kim Arnold

Enterprise Architects
- ***Brett Allport*** *- Customer*
- ***Francis Kaitano*** *- Cybersecurity*
- ***Glenn Bellam*** *– Engineering & App Integration*
- ***Hugh Walcott*** *- IEM*
- ***John Marshall*** *- Infra*
- ***Michael Lomas*** *- FinCrime*
- ***Tracey Davis*** *- Data & Analytics*

Technology Architecture Forum (TAF)

Lee Challoner-Miles
GM Technology – Digital, Data & AI

Damion Riordan
Head of Tech - Data & Analytics Platforms

Alex Dickson
General Manager Analytics & Insights

Sandra Towgood
HO Operations

Roberta Prentice
HO Data Risk

Alex Wardle
DD&A Strategic Initiatives Manager

Anna Tarasoff
General Manager Data

Alan Fowler
Senior Manager Data Mgmt Tooling

Legend

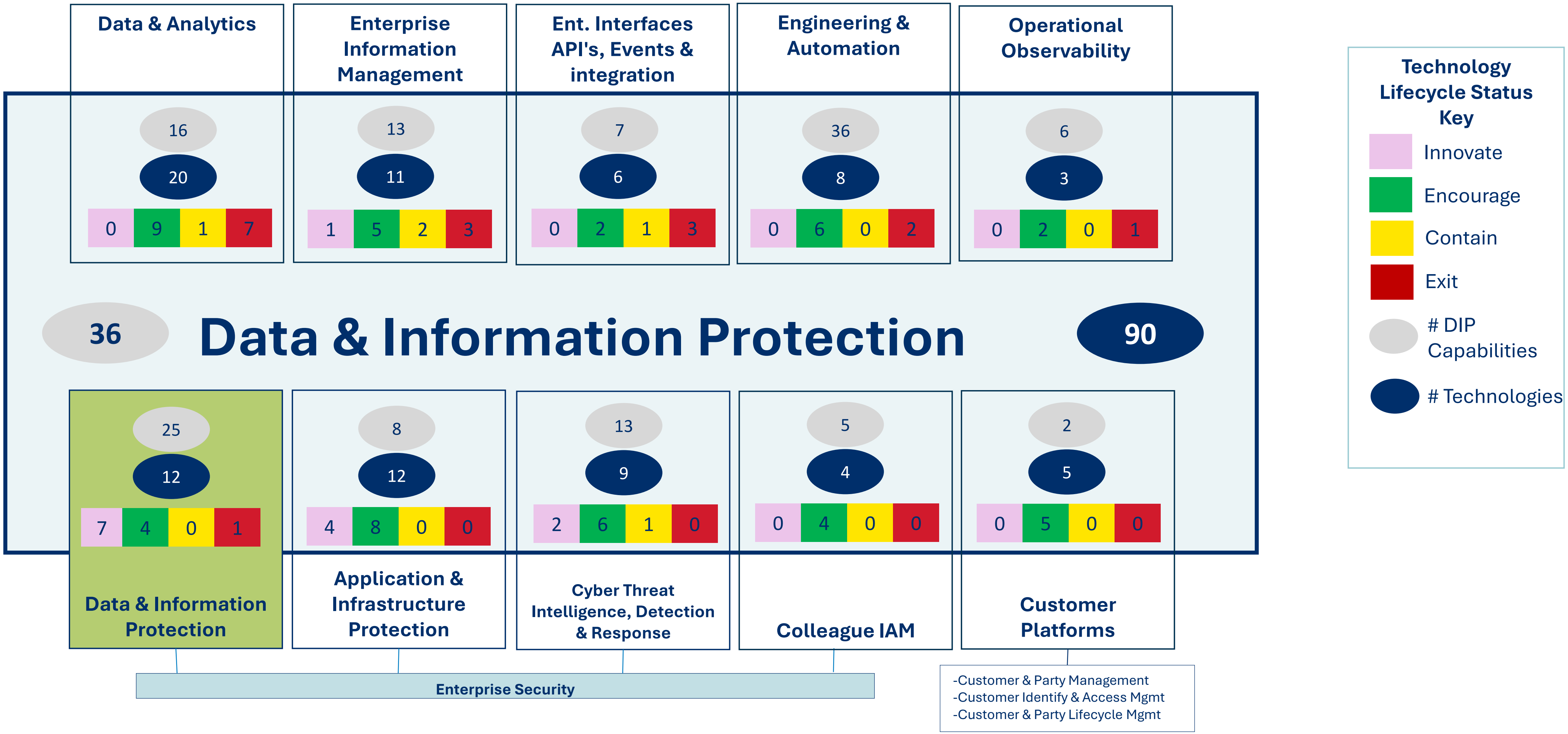
🟧 Enterprise Owners

2. Current State

Current State – Overview

Note – *this is NOT DONE, there are more technologies & platforms to add as we find them*

In protecting data and information across the entire ecosystem, there are many technologies that contribute to Data & Information Protection.



Data & Information Protection

36 (# DIP Capabilities) · 90 (# Technologies)

	# DIP Capabilities	# Technologies	Innovate	Encourage	Contain	Exit
Data & Analytics	16	20	0	9	1	7
Enterprise Information Management	13	11	1	5	2	3
Ent. Interfaces API's, Events & integration	7	6	0	2	1	3
Engineering & Automation	36	8	0	6	0	2
Operational Observability	6	3	0	2	0	1
Data & Information Protection	25	12	7	4	0	1
Application & Infrastructure Protection	8	12	4	8	0	0
Cyber Threat Intelligence, Detection & Response	13	9	2	6	1	0
Colleague IAM	5	4	0	4	0	0
Customer Platforms	2	5	0	5	0	0

Enterprise Security

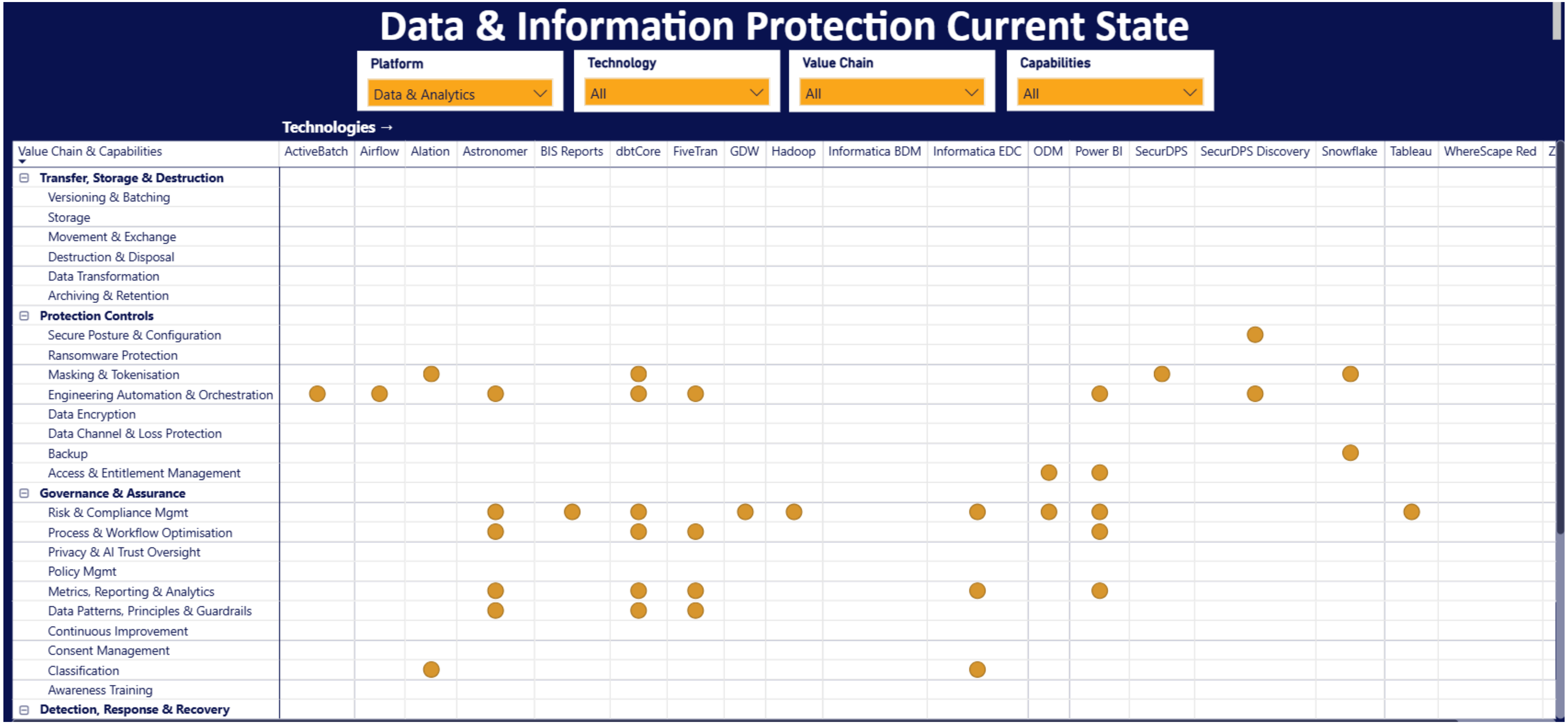
-Customer & Party Management
-Customer Identify & Access Mgmt
-Customer & Party Lifecycle Mgmt

Technology Lifecycle Status Key

- 🟪 Innovate
- 🟩 Encourage
- 🟨 Contain
- 🟥 Exit
- ● # DIP Capabilities
- ● # Technologies

Current State

The technologies across BNZ platforms used to deliver Data & Information Protection today can be visualised by clicking on the report below.



Data & Information Protection Current State

Platform: Data & Analytics

Technology: All

Value Chain: All

Capabilities: All

Technologies →

Value Chain & Capabilities	ActiveBatch	Airflow	Alation	Astronomer	BIS Reports	dbtCore	FiveTran	GDW	Hadoop	Informatica BDM	Informatica EDC	ODM	Power BI	SecurDPS	SecurDPS Discovery	Snowflake	Tableau	WhereScape Red	Z
⊟ **Transfer, Storage & Destruction**																			
Versioning & Batching																			
Storage																			
Movement & Exchange																			
Destruction & Disposal																			
Data Transformation																			
Archiving & Retention																			
⊟ **Protection Controls**																			
Secure Posture & Configuration															●				
Ransomware Protection																			
Masking & Tokenisation			●			●								●		●			
Engineering Automation & Orchestration	●	●		●		●	●						●		●				
Data Encryption																			
Data Channel & Loss Protection																			
Backup																●			
Access & Entitlement Management												●	●						
⊟ **Governance & Assurance**																			
Risk & Compliance Mgmt				●	●	●		●	●		●	●	●				●		
Process & Workflow Optimisation				●		●	●						●						
Privacy & AI Trust Oversight																			
Policy Mgmt																			
Metrics, Reporting & Analytics				●		●	●				●		●						
Data Patterns, Principles & Guardrails				●		●	●												
Continuous Improvement																			
Consent Management																			
Classification			●								●								
Awareness Training																			
⊟ **Detection, Response & Recovery**																			

Challenges

The current state challenges highlight the need to co-ordinate the capabilities across the technology tack to delivery unified Data & Information Protection outcomes.

Fragmented Foundations & Inconsistent Practices

- Legacy tools lack architectural and technical fitness for modern use cases
- Disparate workflows, tools and operating models across domains
- Inconsistent application of policy across technologies
- Lack of standardised protection guardrails and enforcement patterns
- Zero Trust data protection foundational capabilities are missing
- EIM protections are unevenly distributed across systems & lifecycle stages.
- Low maturity enterprise level data detection & response logic.

Operating Model & Capability Maturity

- Operating model is not fit for purpose (DataSecOps, automation, policy)
- Capabilities lack breadth and depth to address excessive and emerging risks
- Conflicting understanding of the risks related to data & information protection across the organisation, and the responsibility for mitigation (e.g. RSK-166 & 171)
- Investment in uplift constrained by prioritisation, resources, and funding.
- Change Management issues – e.g. when rolling out DLP and authentication changes
- Achieving the balance between the need to protect and the need to enable
- Lack of investment and commitment to uplift within the organisation

Governance & Visibility

- Poor end-to-end observability due to fragmented tooling and context sharing
- Gaps for unstructured data in malware protection (outside O365), document disposal and assurance
- Inadequate performance monitoring and governance of document protections
- Unclear data retention and disposal linked to customer lifecycle events
- Limited integration with data catalogue at design time
- Identity and authorisation gaps: unclear access and role-based controls

Culture & Communication

- Perception that Data & Information Protection uplift restricts productivity, leading to push back.
- Technology-led conversations mean we are not leading uplift discussions from the business and customer value perspective
- Lack of data stewardship training and role clarity
- Need for broader communication to build understanding and confidence

3. Platform Target State

Data & Information Protection Modernisation

From Defence to Confidence: Transforming Data & Information Protection into Enterprise Trust & Resilience.

	Cybersecurity-Led *Focused on threat defence, monitoring and incident response*	**Technology Enabled** *Embedded protection in platforms & architecture*	**Enterprise Trust & Resilience** *Unified governance, security, and technology with automation, visibility and strategic alignment*
Industry Trends	**Historic** - Rooted in perimeter defence and reactive models; still relevant but evolving	**Transitional** - Supports modern architectures and automation; needs governance integration to mature.	**Future-facing** - Aligns with trends like zero trust, open banking, AI-driven, automated compliance risk, detection and response.
Drivers	Threat landscape, regulatory pressure, need for resilience and proactive breach readiness	Cloud adoption, automation, agile development, platform modernisation.	Hostile Threat landscape, regulatory compliance, digital transformation, **trust and transparency**.

Transition Pathway →

Key Shifts	- Manual to Automated Controls - Reactive to proactive - Perimeter to identity/data-centric - Siloed to integrated	- Introduces DevSecOps - Automates compliance - Enables real-time monitoring	- Cross-functional ownership - Continuous assurance - Trust and transparency as outcomes - Resilience
Strategic Value	Strong foundation for protection, but limited in agility with digital transformation	Bridges the gap between security and operations; supports scale, agility & cloud first approaches	**Aligns protection with business value and risk appetite. Focussed on enabling and protecting**

Operating Model Shifts

From Defence to Confidence: Transforming Data & Information Protection into Enterprise Trust & Resilience.

	From	To
Customer Centricity	Internal focus on protecting systems and data	External focus on earning trust through transparency and ethical data use
Governance Shift	Isolated within technology/security, with limited visibility across the enterprise	Involve the whole business in trust and resilience, not just technology teams
Strategic Alignment	Security focused on protecting assets and meeting compliance	Trust and resilience part of business strategy and innovation
Scope Expansion	Focus on technical threats, like malware and unauthorised access	Beyond technical threats, to include disruptions, ethics and privacy
Leadership involvement	CISO/Security teams lead, with limited business input	Shared accountability across senior leaders
Cultural Transformation	Security is seen as a blocker or compliance checkbox	Build a culture where everyone trusts, values and protects data & information
Capability Enhancement	Reliance on traditional tools like firewalls, antivirus and access controls	Expand to use advanced tools like data lineage and digital ethics frameworks
Architecture Evolution	Security is added after systems are built (“bolt-on”)	Select and design systems with trust and resilience from the start
Redefined Metrics	Metrics focus on technical indicators (e.g. number of incidents, patching rates)	Measure trust and resilience, not just technical issues

Uplift Themes

Zero Trust by design
Ensure access is granted only when identity, context, and risk are verified—minimising exposure and strengthening resilience.

Continuous Compliance
Embed automated governance and monitoring to maintain real-time assurance and reduce reliance on manual audits.

Privacy First Architecture
Design systems with privacy embedded from the outset, ensuring responsible data use and regulatory alignment.

Secure Data Usage
Enable secure data processing and analytics without compromising sensitive information - unlocking value while protecting trust.

Culture & Capability
Foster a security-aware culture through training, leadership alignment, and integration into operating models.

DataSecOps Driven
Use practices which embed automated security, trust, compliance, workflows and guardrails by design and continuously into every stage of the data lifecycle.

Exceptional Colleague Experiences
Delivering premium user experience, where data and information protection is applied ‘just in time’, lowering friction and toil.

Data & Information Protection – BNZ Vision

Enabling BNZ to move faster, operate safer and lead with confidence in a digital first, regulated world.

From Siloed to Orchestrated Governance

- Implement **federated governance** with shared standards and automation tools—empowering platform teams with guardrails, not gates.
- Establish a **Centre of Enablement** to co-ordinate enterprise-wide protection, trust and resilience

From Independent to Collaborative Delivery

- Shift to an **enterprise shared responsibility model**, enabling teams to own protection outcomes with the right support.
- **Equip and incentivise teams** to prioritise secure configuration and data protection outcomes – not just functional delivery.

From Reactive to Proactive Control

- Embed **automated protection** into the **design and deployment lifecycle**—ensuring controls are integrated from the start, not retrofitted.
- Introduce **automated response workflows** to detect and act on anomalies across platforms.

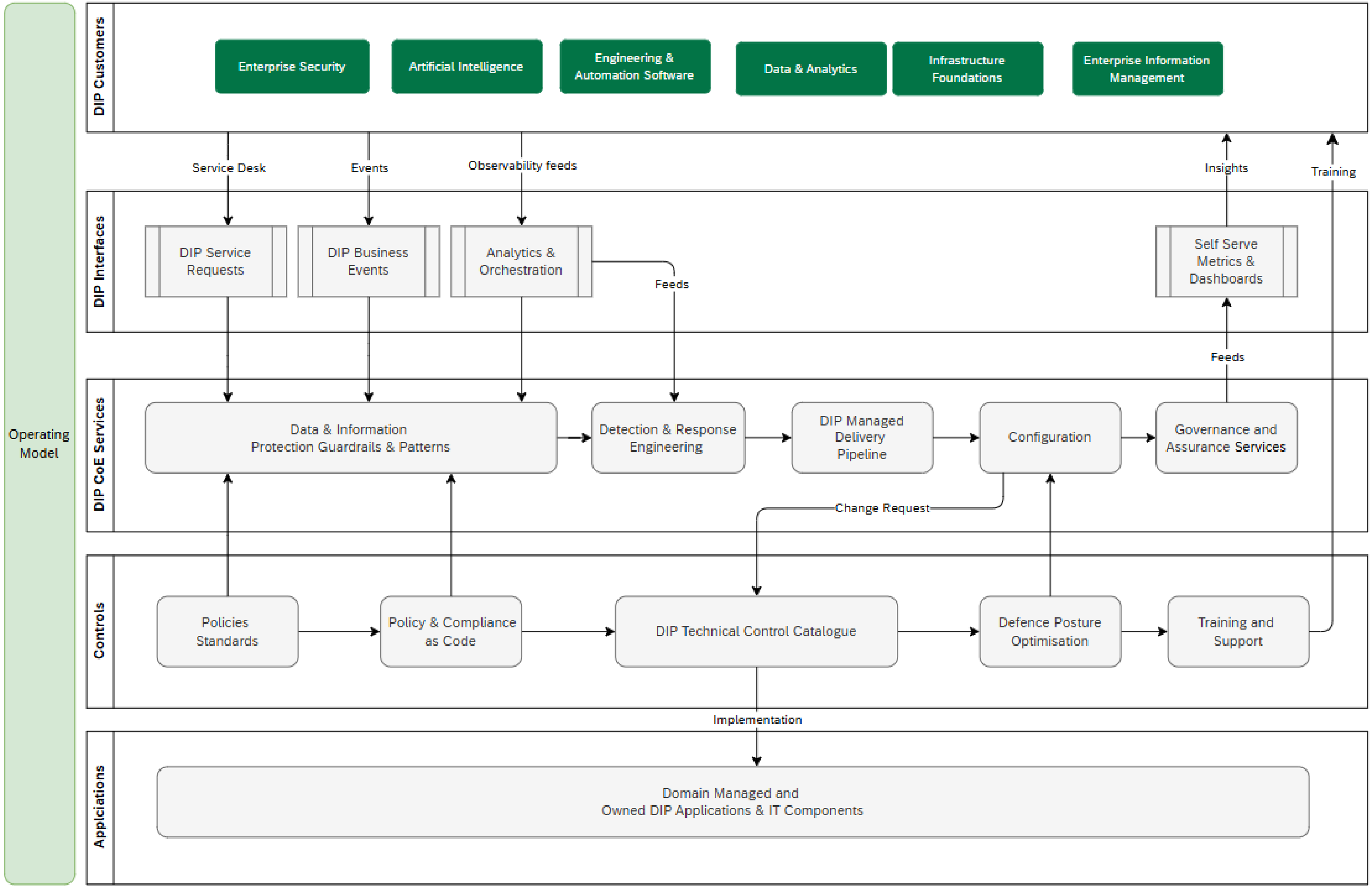
From Tech Uplift to Secure-by-Design

- Leverage existing investment in **cyber**, **cloud transformation** and **data platform modernisation** to embed native protection capabilities.
- Make data protection a **default part of platform engineering**, not an afterthought.

From Cyber-centric to Enterprise Enablement

- Build a **policy translation layer** to convert business protection needs into scalable, platform-specific enforcement.
- Enable **cross-platform visibility and orchestration** to align protection with enterprise priorities and delivery pipelines.

Target State


Operating Model
DIP Customers
Enterprise Security
Artificial Intelligence
Engineering & Automation Software
Data & Analytics
Infrastructure Foundations
Enterprise Information Management
Service Desk
Events
Observability feeds
Insights
Training
DIP Interfaces
DIP Service Requests
DIP Business Events
Analytics & Orchestration
Feeds
Self Serve Metrics & Dashboards
Feeds
DIP CoE Services
Data & Information Protection Guardrails & Patterns
Detection & Response Engineering
DIP Managed Delivery Pipeline
Configuration
Governance and Assurance Services
Change Request
Controls
Policies Standards
Policy & Compliance as Code
DIP Technical Control Catalogue
Defence Posture Optimisation
Training and Support
Implementation
Applciations
Domain Managed and Owned DIP Applications & IT Components

Customer Layer: Platform owners who, through training and insights, can access DIP services via the interface layer.

Interface Layer: Defining how to engage data and information protection platform support and delivery services.

CoE Services Layer: Defines the services available, from prepared patterns, guardrails, to the delivery of configuration changes, recommendations and insights

DIP Control Layer: Catalogue of governed risk mitigations, including policies, standards, training and support.

Application Support Layer: representing the technologies responsible for implementing the configuration changes

4. Roadmap

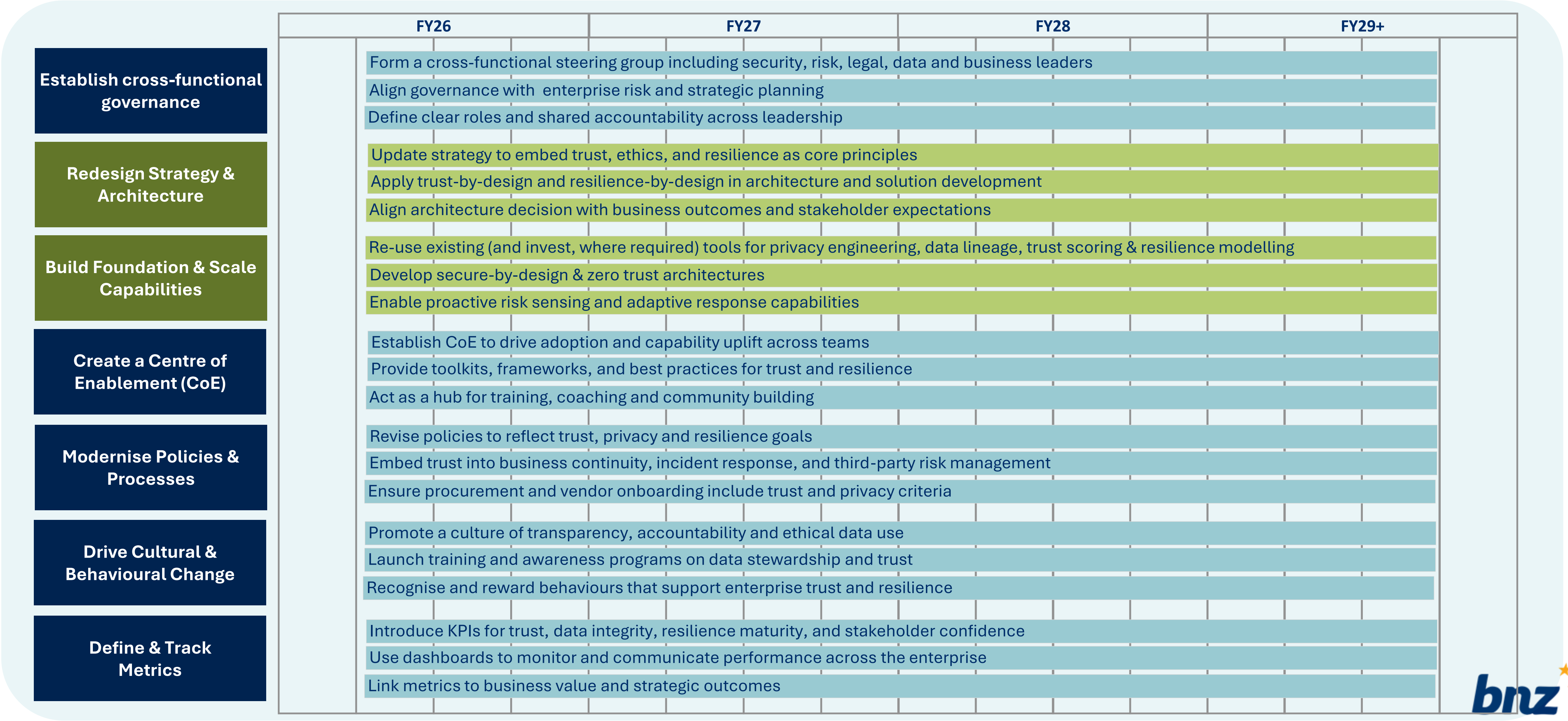
Indicative Roadmap

Indicating the actions needed to evolve our operating model from cybersecurity-led to a trust and resilience driven enterprise approach.

Key

Technology driven

Non Tech



FY26 | FY27 | FY28 | FY29+

Establish cross-functional governance

- Form a cross-functional steering group including security, risk, legal, data and business leaders
- Align governance with enterprise risk and strategic planning
- Define clear roles and shared accountability across leadership

Redesign Strategy & Architecture

- Update strategy to embed trust, ethics, and resilience as core principles
- Apply trust-by-design and resilience-by-design in architecture and solution development
- Align architecture decision with business outcomes and stakeholder expectations

Build Foundation & Scale Capabilities

- Re-use existing (and invest, where required) tools for privacy engineering, data lineage, trust scoring & resilience modelling
- Develop secure-by-design & zero trust architectures
- Enable proactive risk sensing and adaptive response capabilities

Create a Centre of Enablement (CoE)

- Establish CoE to drive adoption and capability uplift across teams
- Provide toolkits, frameworks, and best practices for trust and resilience
- Act as a hub for training, coaching and community building

Modernise Policies & Processes

- Revise policies to reflect trust, privacy and resilience goals
- Embed trust into business continuity, incident response, and third-party risk management
- Ensure procurement and vendor onboarding include trust and privacy criteria

Drive Cultural & Behavioural Change

- Promote a culture of transparency, accountability and ethical data use
- Launch training and awareness programs on data stewardship and trust
- Recognise and reward behaviours that support enterprise trust and resilience

Define & Track Metrics

- Introduce KPIs for trust, data integrity, resilience maturity, and stakeholder confidence
- Use dashboards to monitor and communicate performance across the enterprise
- Link metrics to business value and strategic outcomes

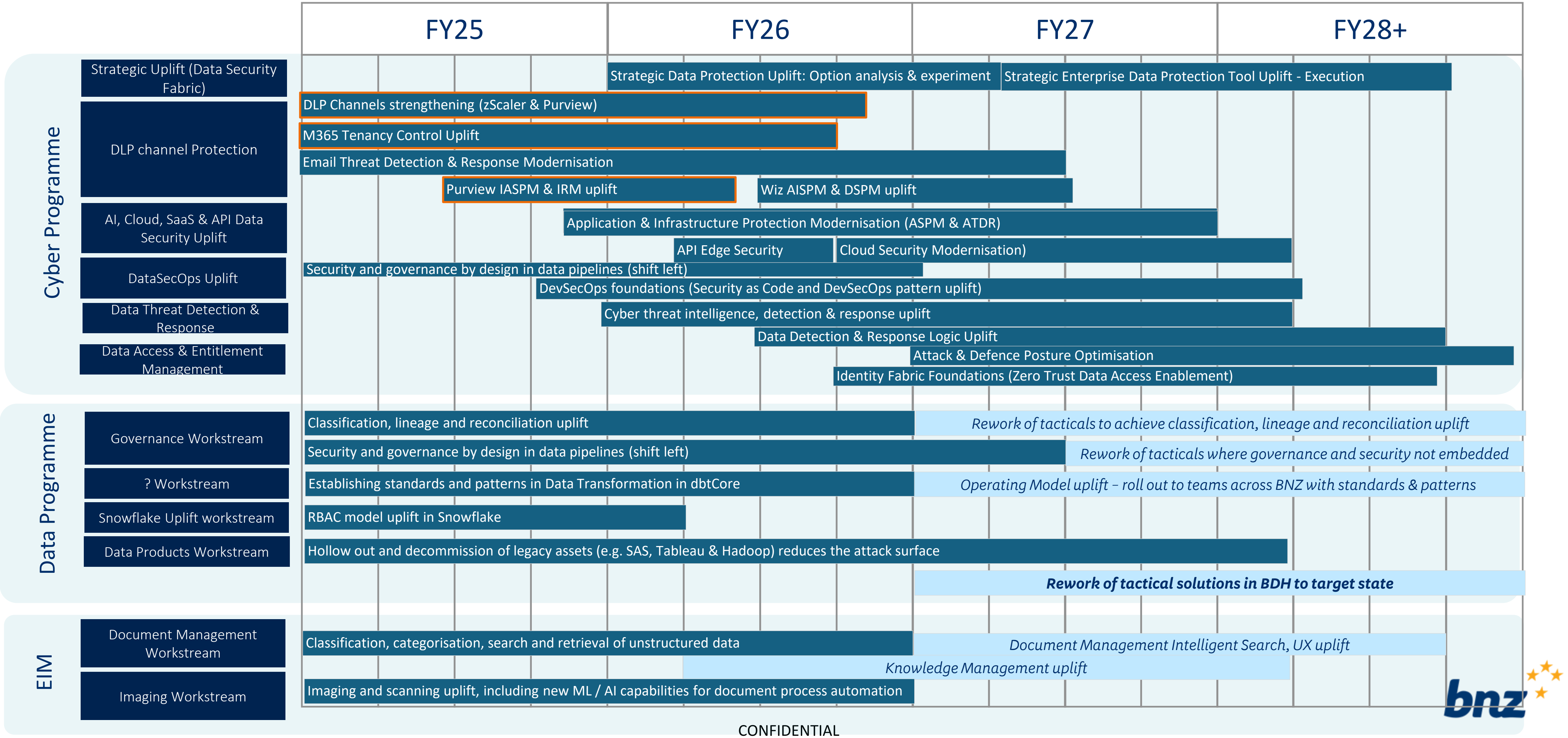
Planned Uplift Roadmap

Investment in other platforms that contribute to Data & Information Protection uplift.

Future investment

Current investment

Revision of Approach Required



FY25 | FY26 | FY27 | FY28+

Cyber Programme

- Strategic Uplift (Data Security Fabric)
  - Strategic Data Protection Uplift: Option analysis & experiment
  - Strategic Enterprise Data Protection Tool Uplift - Execution
- DLP channel Protection
  - DLP Channels strengthening (zScaler & Purview)
  - M365 Tenancy Control Uplift
  - Email Threat Detection & Response Modernisation
  - Purview IASPM & IRM uplift
  - Wiz AISPM & DSPM uplift
- AI, Cloud, SaaS & API Data Security Uplift
  - Application & Infrastructure Protection Modernisation (ASPM & ATDR)
  - API Edge Security
  - Cloud Security Modernisation)
- DataSecOps Uplift
  - Security and governance by design in data pipelines (shift left)
  - DevSecOps foundations (Security as Code and DevSecOps pattern uplift)
- Data Threat Detection & Response
  - Cyber threat intelligence, detection & response uplift
  - Data Detection & Response Logic Uplift
  - Attack & Defence Posture Optimisation
- Data Access & Entitlement Management
  - Identity Fabric Foundations (Zero Trust Data Access Enablement)

Data Programme

- Governance Workstream
  - Classification, lineage and reconciliation uplift
  - *Rework of tacticals to achieve classification, lineage and reconciliation uplift*
  - Security and governance by design in data pipelines (shift left)
  - *Rework of tacticals where governance and security not embedded*
- ? Workstream
  - Establishing standards and patterns in Data Transformation in dbtCore
  - *Operating Model uplift – roll out to teams across BNZ with standards & patterns*
- Snowflake Uplift workstream
  - RBAC model uplift in Snowflake
- Data Products Workstream
  - Hollow out and decommission of legacy assets (e.g. SAS, Tableau & Hadoop) reduces the attack surface
  - ***Rework of tactical solutions in BDH to target state***

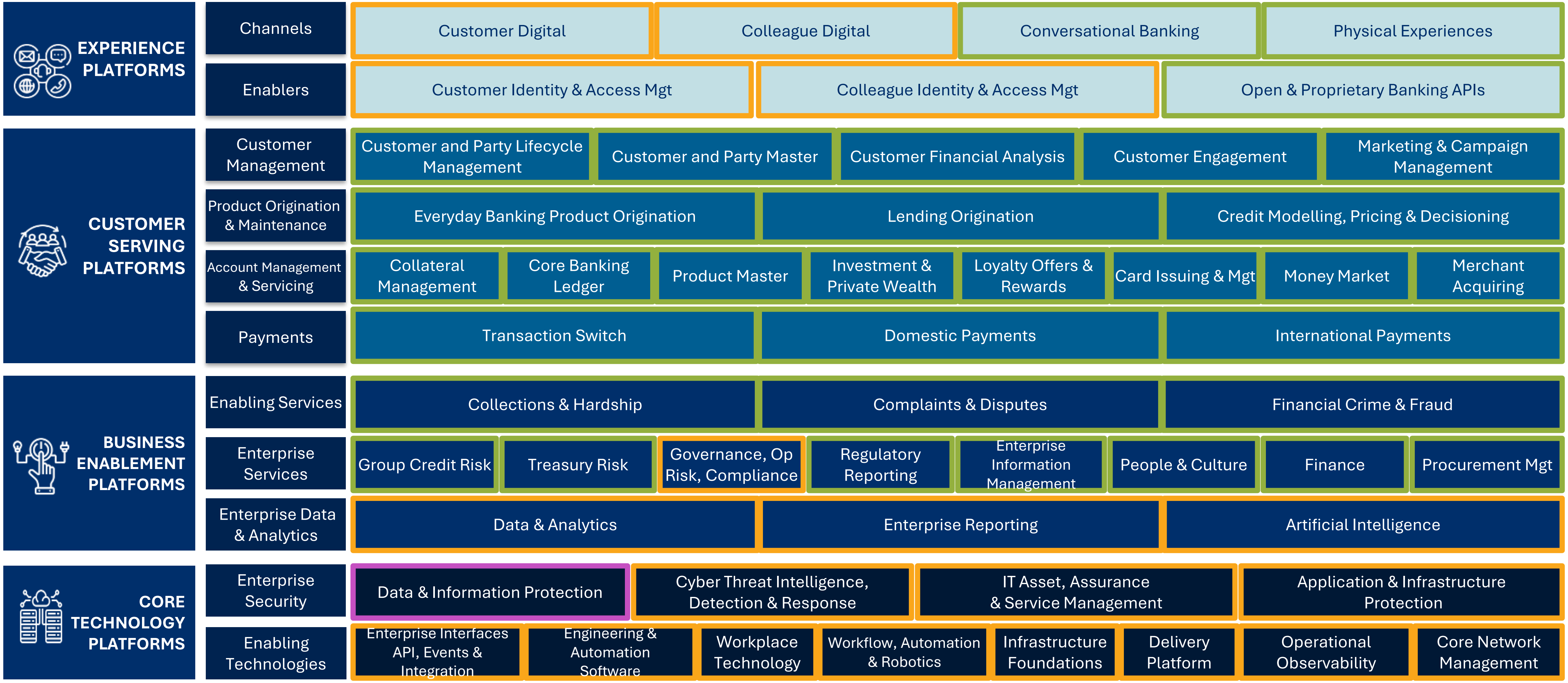
EIM

- Document Management Workstream
  - Classification, categorisation, search and retrieval of unstructured data
  - *Document Management Intelligent Search, UX uplift*
  - *Knowledge Management uplift*
- Imaging Workstream
  - Imaging and scanning uplift, including new ML / AI capabilities for document process automation

Platforms @ BNZ

A key theme of the bank's Technology Strategy is to adopt a platform mindset that will help transform the bank with our Intentional Modernisation approach.

Platform in scope is highlighted in **plum**, Up-stream dependencies are highlighted **lime**, Down-stream dependencies are highlighted **orange**.



EXPERIENCE PLATFORMS

- Channels: Customer Digital; Colleague Digital; Conversational Banking; Physical Experiences
- Enablers: Customer Identity & Access Mgt; Colleague Identity & Access Mgt; Open & Proprietary Banking APIs

CUSTOMER SERVING PLATFORMS

- Customer Management: Customer and Party Lifecycle Management; Customer and Party Master; Customer Financial Analysis; Customer Engagement; Marketing & Campaign Management
- Product Origination & Maintenance: Everyday Banking Product Origination; Lending Origination; Credit Modelling, Pricing & Decisioning
- Account Management & Servicing: Collateral Management; Core Banking Ledger; Product Master; Investment & Private Wealth; Loyalty Offers & Rewards; Card Issuing & Mgt; Money Market; Merchant Acquiring
- Payments: Transaction Switch; Domestic Payments; International Payments

BUSINESS ENABLEMENT PLATFORMS

- Enabling Services: Collections & Hardship; Complaints & Disputes; Financial Crime & Fraud
- Enterprise Services: Group Credit Risk; Treasury Risk; Governance, Op Risk, Compliance; Regulatory Reporting; Enterprise Information Management; People & Culture; Finance; Procurement Mgt
- Enterprise Data & Analytics: Data & Analytics; Enterprise Reporting; Artificial Intelligence

CORE TECHNOLOGY PLATFORMS

- Enterprise Security: Data & Information Protection; Cyber Threat Intelligence, Detection & Response; IT Asset, Assurance & Service Management; Application & Infrastructure Protection
- Enabling Technologies: Enterprise Interfaces API, Events & Integration; Engineering & Automation Software; Workplace Technology; Workflow, Automation & Robotics; Infrastructure Foundations; Delivery Platform; Operational Observability; Core Network Management

NAB Alignment

NAB haven't adopted Data & Information Protection as a platform, however the approach is similar. NAB includes the higher level BIAN capabilities for Data & Information Protection into other platforms while BNZ aggregates lower level capabilities into Data & Information Protection. BNZ & NAB are targeting similar outcomes across contributing platforms e.g. secure-by-design, proactive risk and threat informed protection.

- NAB have instead built the (higher level) BIAN capabilities that cover Data & Information Protection into other platforms, such as:

  Storage & Data Protection, Data Archiving & Records Management
  Governance, Compliance & Risk (breach reporting)
  Workflow Process Automation
  Security Services

It could be useful to map the lower level capabilities in BNZ Data & Information Protection to the higher level BIAN capabilities and draw out the similarities and differences further.

The Data & Information Protection at BNZ does not neatly align to NAB's definition of platform – while it has a well defined capability boundary it is an aggregation, the proposal is an aggregate of technologies that sit in other platforms. The responsibility for technology within the platform is therefore challenging, because on it's own Data & Information Protection won't have any technologies.

NAB's Data Protection Team are still taking the cyber centric approach for the next 12 -18 months. Overall, **we align on capabilities and outcomes**.

A further question to ask and answer - Why is Data & Information a platform at BNZ, but not for NAB?

Consulted:

- *John Roome @ NAB*
- *Sam Siggins Lead Domain Architect – Data Security*
- *Karan Narad – Head Of Data Security*

Strategic Alignment

This target state is architected in alignment with BNZ Strategic Ambition through Technology Themes and Intentions.

Our goal is to be New Zealand's
best bank
in personal and business.
colleagues and customers.
Perfect the basics
Build strong foundations
Deliver market-leading experiences
How we'll do it is by living our Mātāpono

Modernise and Simplify

Objective: Intentional simplification and modernisation.

Approach

- **Getting the Basics Right:** Significantly reduced tool landscape, functional overlap and complexity.
- **Laying the Right Foundations:** Modernise and build missing capabilities required to deliver value stream and target state.
- **Fit for purpose capabilities**: Enable capabilities that are fit for purpose guided by the TSA and the reference blueprint.

Agile and Adaptable

Leveraging **Engineering & DataSecOps** approaches to ensure that the bank is positioned to build and deploy controls y with minimal manual steps by **automating and orchestrating security using context** to invoke the right testing and remediation.

- Shift from reactive to proactive Data & Information Protection.
- Embed and automate detection & response.
- Data & Information Protection as an enabler - Guardrails, not gates

Platform Mindset

We will deliver a composable, well-architected, engineered, and automated platform.

- Simplify by aggregating data & information protection capabilities across existing platforms, rather than a platform on its own.
- Extend capability coverage to have breadth, depth and reach across all the BNZ distributed environments

Resilient, Secure and Safe

Deliver capabilities which enables:

- Shifting from reactive to proactive Data & Information Protection
- Adaptive Posture Refinement.
- Close to real-time security observability.
- Compliance and Secure by design.

Deeply Digital

- Manual touch points will be limited with **flow through automation favoured**.
- Just in time access to data delivering exceptional colleague experiences.
- Use of automation and orchestrations consistently across the DIP ecosystem.

5. Risk Overview of Current State

Current State – Business Risk

The following GRACE risks are impacted by the Data & Information Protection Platform.

Risk Summary	TSA Impact Description	TSA Impact to Risk Profile
RSK- 171: Cyber Compromise Risk There is a risk that information systems containing customer, employee or business data lose their confidentiality, integrity, or availability. Due, but not limited to, inappropriate or excessive access to systems or data; malware or ransomware attack; espionage, hacktivism or supply chain breach; inadequate patch and vulnerability management; malicious insider intent or human error; compromised credentials; insecure coding practices; unauthorised asset or environment changes; lack of asset ownership; insecure service configuration; third party compromise; sophisticated use of artificial intelligence by threat actors; and asset currency.	This TSA is responsible for building and delivering the key foundational capabilities and controls for enabling to mitigate this risk and managing the need for having the ability to proactively detect, respond and contain cyber compromises. Current capabilities are rudimentary and requires significant uplift in order to transition to a fit for purpose target state which is fit for purpose to reduce the residual risk.	Direct Risk Buydown
RSK-166 Data Loss This risk focuses on unauthorised access to BNZ data in electronic or physical format (customer, employee and any intellectual property) resulting in loss or disclosure of BNZ confidential information.	Capabilities and controls delivered through the target state directly impacts our ability to proactively detect, respond and contain any risks, threats, and breaches associated with data breaches. Current capabilities are rudimentary and require significant uplift in order to transition to a fit for purpose target state which is fit for purpose to reduce the residual risk.	Directly Impacts Risk Mitigation
RSK-158 IT System Failure The risk focuses on the failure to properly manage BNZ Information Technology (IT) assets (infrastructure, applications and systems) and effectively respond to IT incidents resulting in service outages and disruptions.	Cyber incidents, such as **Denial of Services (Volumetric) and Ransomware** attacks, are on the rise and usually result in system failure and outages when they occur. The TSA contributes to minimisation of this risk delivering autonomic cyber defence capabilities which are fit for purpose to mitigate our exposure to cyber threats. Modernisation will also result in simplification and optimisation of tools, reducing the number of technologies and environments to manage and maintain.	Directly Impacts Risk Mitigation

Current State – Business Risk

The following GRACE risks are impacted by the Data & Information Protection Platform.

Risk Summary	TSA Impact Description	TSA Impact to Risk Profile
RSK-1300 Data Management Risk Data management risk is the risk that data / information / records is incorrect (incomplete, inaccurate, inaccurately transformed), or is incorrectly used (inappropriate use, unethical use, use breaching confidentiality or privacy, outputs not fit for purpose, incorrectly disposed).	The TSA positively impacts Data Risk 4 - Inappropriate or unethical use of data (incorrect use of data). Reducing overcollection, through appropriate classification and enabling appropriate retention and disposal. Through reduced opportunity for unauthorised manipulation and alteration of data and in applying appropriate protection (masking/tokenisation etc) for sensitive data. The observability in the target state allows identification and resolution, where overcollection occurs and where sensitive data is found to be unprotected.	Direct Risk Buydown
RSK-1288 Issuing and Acquiring Compliance Risk There is a risk of failure to: • Comply with Payment Card Industry Data Security (PCI DSS) and its encompassing requirements • Comply with Card Scheme requirements (issuing & acquiring), including transaction processing, authorisation & settlement requirements, interchange, transaction recording and record keeping (Card Schemes - Visa, Mastercard, Amex, UnionPay and Alipay). • Comply with Payments NZ Industry rules and procedures • Manage appropriately merchant acquiring customer and exposure risk, *excluding the management of merchant product/systems and fraud risk*	Capabilities and controls delivered through the target state directly impacts our ability to proactively deliver the control efficacy required to meet with the PCI DSS data security requirements and to reduce the residual risk of non compliance. Capabilities delivered will also enhance our abilities to protect customer and card payments data.	Directly Impacts Risk Mitigation

6. Focus Areas

Technical Focus Areas

To support the move towards the proposed target state, the following focus areas have been identified as relevant, either as foundational enabling aspects or unknown areas that would require further refinement.

Zero-Trust Architecture

Shift an identity & trust based architecture – dynamic and risk based access

- **Verify every access** no user or device is trusted by default, even inside the network
- **Enforce least privilege** Grant only the minimum access needed for each request
- **Continuously validate trust** monitor and re-authenticate dynamically
- **Secure across boundaries** apply consistent controls across cloud, on-prem and hybrid

Event-driven and decoupled systems security

Enhancing resilience by securing service interactions, protecting data, detecting anomalies and maintaining accuracy

- **Limit breach impact** Decoupled systems isolate vulnerabilities
- **Enable real-time alerts** Event-driven models that allows instant threat detection
- **Enforces Zero-Trust-** Each service manages its own access controls
- **Boosts Resilience** Systems recover independently and securely

Synthetic Data & Data Simulation

Agentic AI to generate synthetic data for testing & training?

- **Protect privacy** Generate realistic data without exposing sensitive info
- **Enable safe testing** support secure testing and training without using prod data
- **Speed up development** remove data access barriers, allow faster innovation and prototyping
- **Improve security validation** simulate edge cases to test and strengthen data protection controls

Data Detection & Response Uplift

Proactive detection & response to threats and breaches

- **Proactively identify threats** Advanced analytics/AI to detect suspicious activity before damage occurs
- **Accelerate incident response** Enables rapid containment and remediation of breaches
- **Improved visibility** Enhanced monitoring across data flows, endpoints and cloud environments
- **Support continuous protection** Integrate with security ops for real-time threat management

Data Security Posture & Configuration

Automation of capabilities responsible for identifying exposures and misconfiguration across data assets, and their mitigations

- **Automate exposure detection** Continuously scan for misconfiguration & vulnerabilities across data assets
- **Prioritises risk mitigation** Flags high risk issues and recommends target remediation actions
- **Improves visibility** Centralised insight into data security posture across environments
- **Policy enforcement** Aligns config with security policy & compliance standards

Channel Loss Prevention

Strengthening breadth and coverage across channels

- **Expand Coverage** Strengthens monitoring across all communication and data transfer channels
- **Detect Data Leakage** Identify unauthorised or accidental data exfiltration in real time
- **Apply consistent controls** Enforces data protection policies across email, web, cloud and endpoint channels
- **Reduces insider risk** Monitors user behaviour to prevent intentional or unintentional data loss

Future Focus Areas

In addition to current focus areas, the following future-focussed areas are emerging considerations that may not require immediate action but warrant ongoing attention and strategic foresight.

AI Readiness

** Will be covered in AI TSA*

Prepare to safely and effectively adopt and scale AI technologies

- **Establish data governance** Ensure integrity, privacy and security in AI systems
- **Enable risk monitoring** continuously audit AI deployments for potential threats
- **Promote ethical AI use** train stakeholders on responsible AI practices
- **Build scalable infrastructure** distributed, fault tolerant systems that maintain data integrity and availability under load

AI Opportunities

Understand how AI can enhance Data & Information Protection

- **Detect threats early** identify anomalies and suspicious behaviour in real-time
- **Classify sensitive data** automate tagging and access control based on risk
- **Protect privacy** enable techniques like synthetic data and differential privacy
- **Predict risks a**nticipate vulnerabilities through behavioural and historic analysis

Privacy-enhancing technologies

Trusted execution environments to protect sensitive data and code during processing

- **Secures data in use** protect sensitive data during processing, not just at rest or in transit
- **Isolates execution** runs code in secure, tamper-resistant environments
- **Prevents unauthorised access** blocking external threats from accessing protected workloads
- **Supports compliance** enables secure processing aligned with privacy regulations.

Post Quantum cryptography

As quantum computing advances, traditional encryption methods may become vulnerable

- **Prepare for Quantum threats** anticipate future risks to current encryption methods
- **Secure Long-term Data** protect sensitive data that must remain confidential for decades
- **Enable cryptographic transition** support migration to quantum-resistant algorithms
- **Maintain compliance** align with emerging standards for post-quantum security

Data sovereignty & cross border compliance

Architect to account for data residency, support geo-fencing and enable jurisdiction aware data handling

- **Data residency** ensure data is stored and processed within approved jurisdictions
- **Enable geo fencing** restrict data access and movement based on geographic boundaries
- **Implement jurisdiction awareness** adapt data handling to comply with local laws and regs
- **Mitigates legal risk** reduces exposure to cross-border data transfer violations

Resilience against ransomware & data tampering

Confidential computing, immutable storage, air-gapped backups and recovery architecture. Blockchain for tamper-evident logs

- **Prevent alteration** through **confidential computing,** immutable storage to block unauthorised changes.
- **Ensure recovery** Maintain attested backups and resilient recovery architecture.
- **Detect tampering** leverage blockchain for tamper-evident logging and audit trails.
- **Browser as the last mile:** Bolstering browser protection to mitigate against browser driven data and AI threats.

Next Steps

To support the move towards the proposed target state, the following next steps are recommended.

Data & Information Protection as a platform?

Consider whether D&IP as a sub-platform of Security is appropriate? Or if Data & Information Protection as a platform is appropriate at all?

- The target state demonstrates how DIP is delivered outside of a specific platform.
- Does BNZ have the scale and investment to support dropping the platform in alignment with NAB?
- The apps within the current DIP platform can be collapsed into existing platforms – may drive slight changes to naming & boundaries of existing platforms

Operating Model

A more holistic and strategic focus, requires significant operating model change

- RACI to clarify roles, boundaries and responsibilities.
- Building the capacity to enable an engineering centric operating model, right sized to deliver DataSecOps .
- Who owns the blueprint for delivering the uplift and the ongoing currency?

Exec Buy in

Commitment & investment is required from BNZ leaders

- Cross-functional leadership – CIO, DD&A, legal, risk and business. Governance is integrated into enterprise risk and strategic planning
- Overarching accountability for the existing Excessive data risks e.g.: RSK- 166, 171, RKS 1288, etc.
- Approach for driving investments to deliver the target state uplift and outcomes.

Principles, Practices & Patterns

The foundations and scaffolding for Data & Information Protection uplift

- Defining the structure for core enabling tools.
- Establishment of patterns and guardrails for enabling coherence.
- Codification and standardisation of guardrails, standards and policies.
- Automation and Orchestration of controls and workflows.

Appendices

Value Chain & Capability Definitions

	Capability	Description
Data Discovery & Classification Processes and tools that help identify, catalog, and classify data based on its sensitivity, criticality, and business value. This enables appropriate protection and governance measures to be applied.	Classification	Categorising data and information assets based on sensitivity and criticality to apply appropriate protection measures
	Data Business Rules Mgmt & Refinement	Managing and refining business logic applied to data and information assets, for example data transformation or metadata used for data protection.
	Data Catalog	Centralized inventory of data and information assets to support discovery, governance, and access control.
	Data Lineage	Tracking the origin, movement, and transformation of data and information assets across systems.
Protection Controls Technical and procedural safeguards that prevent unauthorised access, disclosure, alteration, or destruction of data. These include encryption, access controls, and secure configurations.	Access & Entitlement Management	Controlling who can access data and what actions they can perform.
	Backup	Creating periodic copies of data to recover in case of loss or corruption.
	Data Channel & Loss Protection	Preventing unauthorized and unintentional data transmission and leakage.
	Data Encryption	Securing data by converting it into unreadable format without proper keys.
	Engineering Automation & Orchestration	Automating and embedding security, responses and workflows.
	Masking & Tokenisation	Obscuring sensitive data to reduce exposure risk during processing or testing.
	Ransomware Protection	Defending against malicious software that encrypts data for ransom.
	Secure Posture & Configuration	Ensuring systems are securely configured to prevent vulnerabilities.
Governance & Assurance Policies, roles, oversight mechanisms, and continuous improvement practices that ensure data protection is embedded in organisational culture and aligned with regulatory and business requirements	Awareness Training	Educating staff on data protection policies and practices.
	Consent Management	Ensuring that individuals have control over how their personal data is collected, used, shared, and retained
	Continuous Improvement	Iteratively enhancing data protection capabilities.
	Data Patterns, Principles & Guardrails	Defining consistent rules and standards for data usage and protection.
	Metrics, Reporting & Analytics	Measuring and analysing data protection performance.
	Policy Mgmt	Defining and enforcing rules for data security and privacy.
	Privacy & AI Trust Oversight	Ensuring responsible use of personal data and AI systems.
	Process & Workflow Optimisation	Framework for ensuring the ongoing improvement of data protection processes and workflows for efficiencies and completeness.
	Risk & Compliance Mgmt	Monitoring and managing risks to meet regulatory requirements.

Value Chain & Capability Definitions Cont…

	Capability	Description
Transfer, Storage & Destruction Controls and practices that govern how data is securely stored, moved, retained, and ultimately disposed of, ensuring lifecycle integrity and compliance with legal and operational standards.	Archiving & Retention	Preserving data for legal, regulatory, or operational needs.
	Data Transformation	Modifying data formats securely during processing.
	Destruction & Disposal	Securely eliminating data that is no longer needed.
	Movement & Exchange	Securing data as it moves(in motion) or as it is exchanged between different parties with varying risk or trust levels.
	Storage	Securely maintaining data in physical or cloud environments.
	Versioning & Batching	Managing data changes and grouping for efficient processing.
Detection, Response & Recovery Capabilities that enable the organization to detect threats, respond to incidents, and recover from data breaches or system failures, minimizing impact and restoring normal operations.	Behavioural & Activity Monitoring	Observing user and system behaviour to detect anomalies.
	Data Breach Analysis & Response	Investigating and mitigating data breaches.
	Data Incident Playbooks	Predefined procedures for responding to data security incidents.
	Data Quality	Observing that information is accurate, complete, and consistent—making it easier to detect anomalies, prevent breaches, and enforce access controls effectively.
	Data Recovery & Restoration	Restoring data after loss or compromise.
	Data Threat Monitoring & Orchestration	Identifying and coordinating responses to threats.
	Data Vulnerability & Exposure Mgmt	Identifying and mitigating weaknesses in data systems.
	Forensics Analysis & Investigation	Examining incidents to understand root causes and impacts.
	Performance Monitoring	Tracking system performance to detect potential security issues.

Stakeholder Engagement

Date	Stakeholders	Description
25/8/25	Rodger Donaldson, Paul Dudding	Data platform architects run through & updates
26/8/25	Shirley McIntyre, Tanya Boelema, Ann Tiatia	GM Tech Strategy & Architecture, HoA engagement
27/8/25	Dan Williams, Grace Shin, Dan Dove, Rebecca Mursell, Alan Fowler	Key DD&A people in data engineering, data risk, data governance
27/8/25	David Grant	DD&A Advanced Analytics – high level sharing
28/8/25	Anna Tarasoff, Roberta Prentice, Alex Dickson	DD&A GMs & data risk
29/8/25	Lee Challoner-Miles	GM Data, Digital & AI
1/9/25	Nic Olivier	GM briefing – short run through exec pack
1/9/25	Kim Arnold	HoA engagement
5/9/25	Richard Boxall, Brett Williams, Mrinal Mukherjee	CISO, HO and Product Manager
5/9/25	Damion Riordan, Deb Gill, Jane Eagle, Haseeb Quazi, Dave Dyer	DAP LT
8/9/25	Sandra Towgood, Alex Wardle	DD&A leaders
12/9/25	Mrinal Mukherjee, Diego McCormic, Karl Lellman, Red Hanlon	Cyber Data Protection Team & Security Architects
15/9/25	Hayden Smith, Oliver Jennings, Bianca Collor, Francois Herbert	Engineering HO and Product Managers
16/9/25	Kate Skinner	Exec briefing
23/9/25	Cross Domain (Strategy & Architecture, DD&A, Cyber and Core) GMs	Workshop with the key cross functional GMs to discuss and clarify Operating Model, Boundaries and Approach.

User Perspective

- I want it to "just work"
- I want it to be easy to do the right thing
- I want to know the data is secure
- I have an obligation to treat data securely

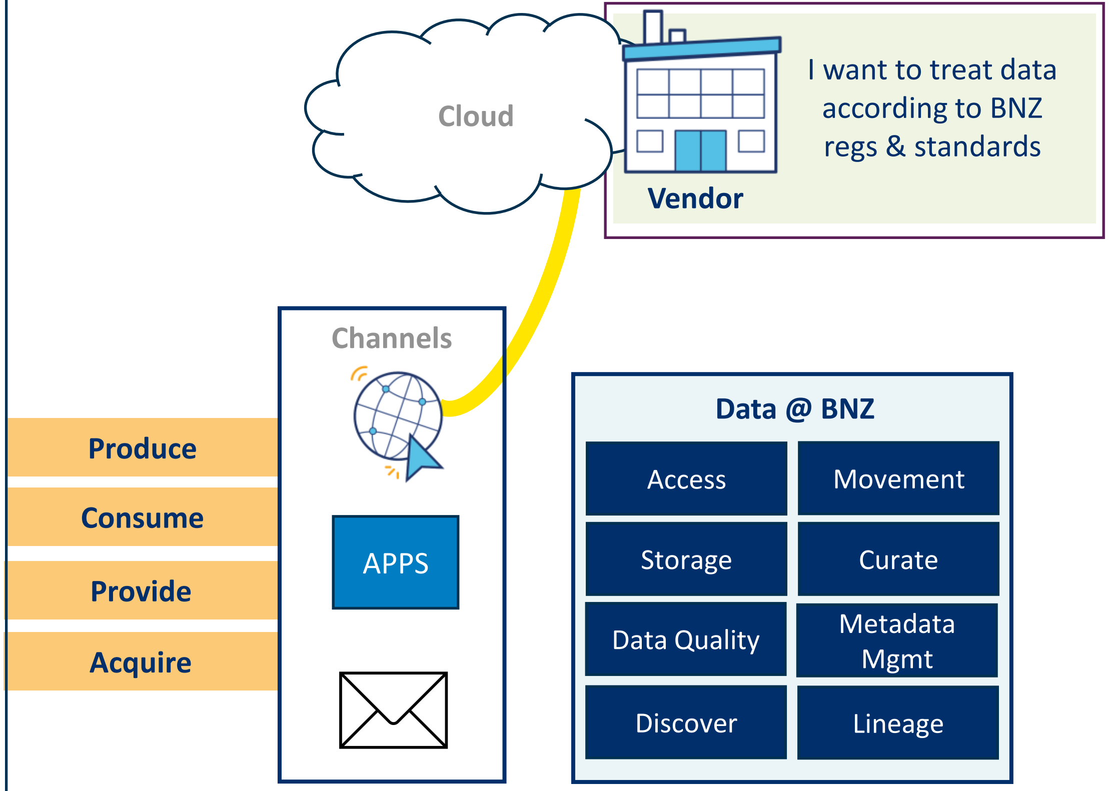
Colleague

- I want it to "just work"
- I want to trust my bank
- I need guidance in how to keep my data safe
- I want to know that the data I produce, provide and access is secure

Customer

- I want to have agreement with BNZ as to how data is accessed and used
- I want easy and secure ways to access data
- I want easy & secure ways to acquire and provide data

Party*



I want to treat data according to BNZ regs & standards

Data @ BNZ

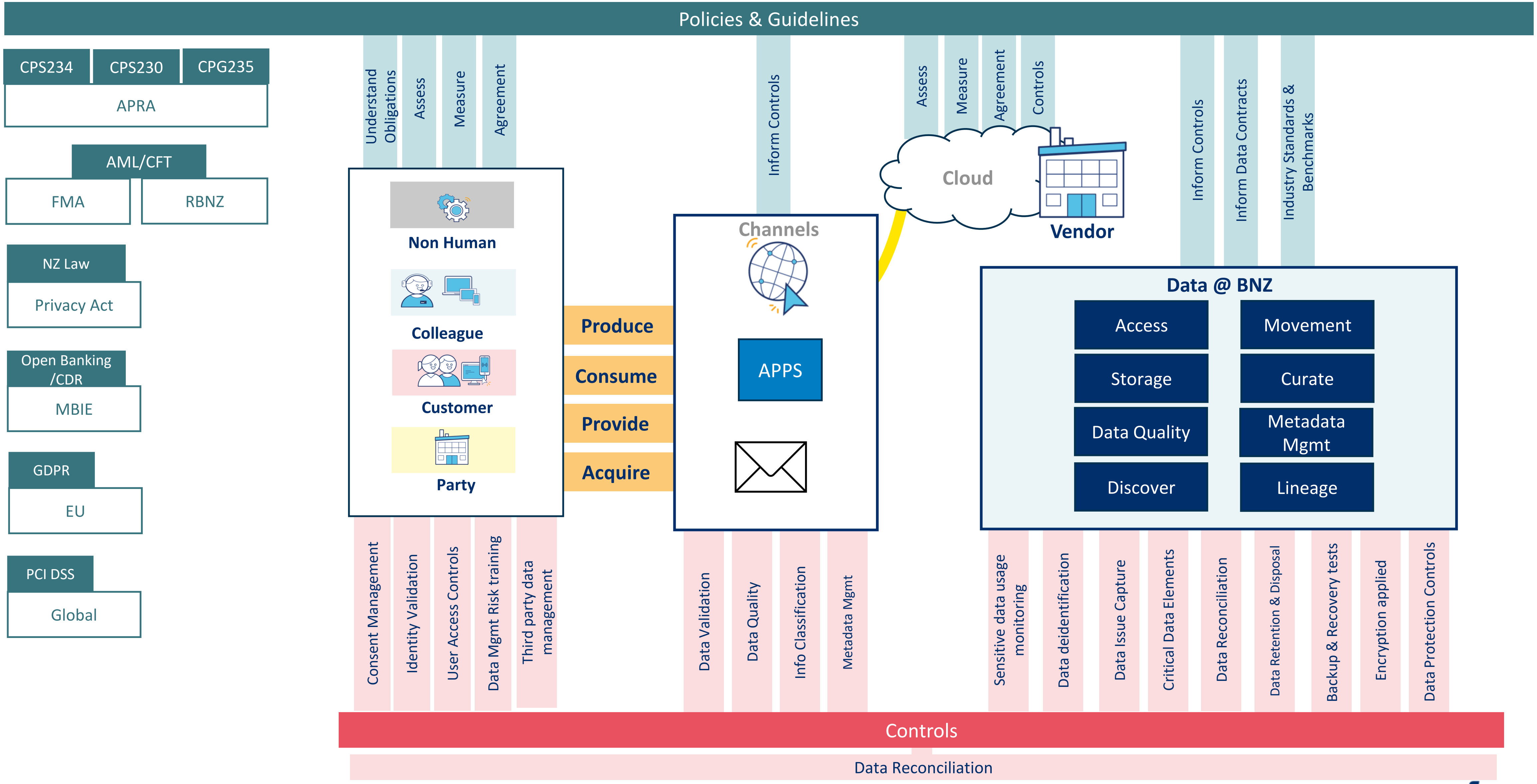
Access	Movement
Storage	Curate
Data Quality	Metadata Mgmt
Discover	Lineage

Data Capture	
Produce	Create data & information
Consume	Use data for business value

Data Distribution	
Provide	Supply data or information that has already been created
Acquire	Acquire data that is already created

Party - Prospects, Partners, Regulatory bodies, vendors, etc. *Note that vendor is called out explicitly here, because the governance of a vendor is different to other parties – per the next slide.*

Governance Perspective



Policies & Guidelines

CPS234 | CPS230 | CPG235

APRA

AML/CFT

FMA | RBNZ

NZ Law

Privacy Act

Open Banking /CDR

MBIE

GDPR

EU

PCI DSS

Global

Understand Obligations | Assess | Measure | Agreement

Non Human

Colleague

Customer

Party

Produce

Consume

Provide

Acquire

Consent Management | Identity Validation | User Access Controls | Data Mgmt Risk training | Third party data management

Inform Controls

Channels

APPS

Data Validation | Data Quality | Info Classification | Metadata Mgmt

Assess | Measure | Agreement | Controls

Cloud

Vendor

Inform Controls | Inform Data Contracts | Industry Standards & Benchmarks

Data @ BNZ

Access | Movement

Storage | Curate

Data Quality | Metadata Mgmt

Discover | Lineage

Sensitive data usage monitoring | Data deidentification | Data Issue Capture | Critical Data Elements | Data Reconciliation | Data Retention & Disposal | Backup & Recovery tests | Encryption applied | Data Protection Controls

Controls

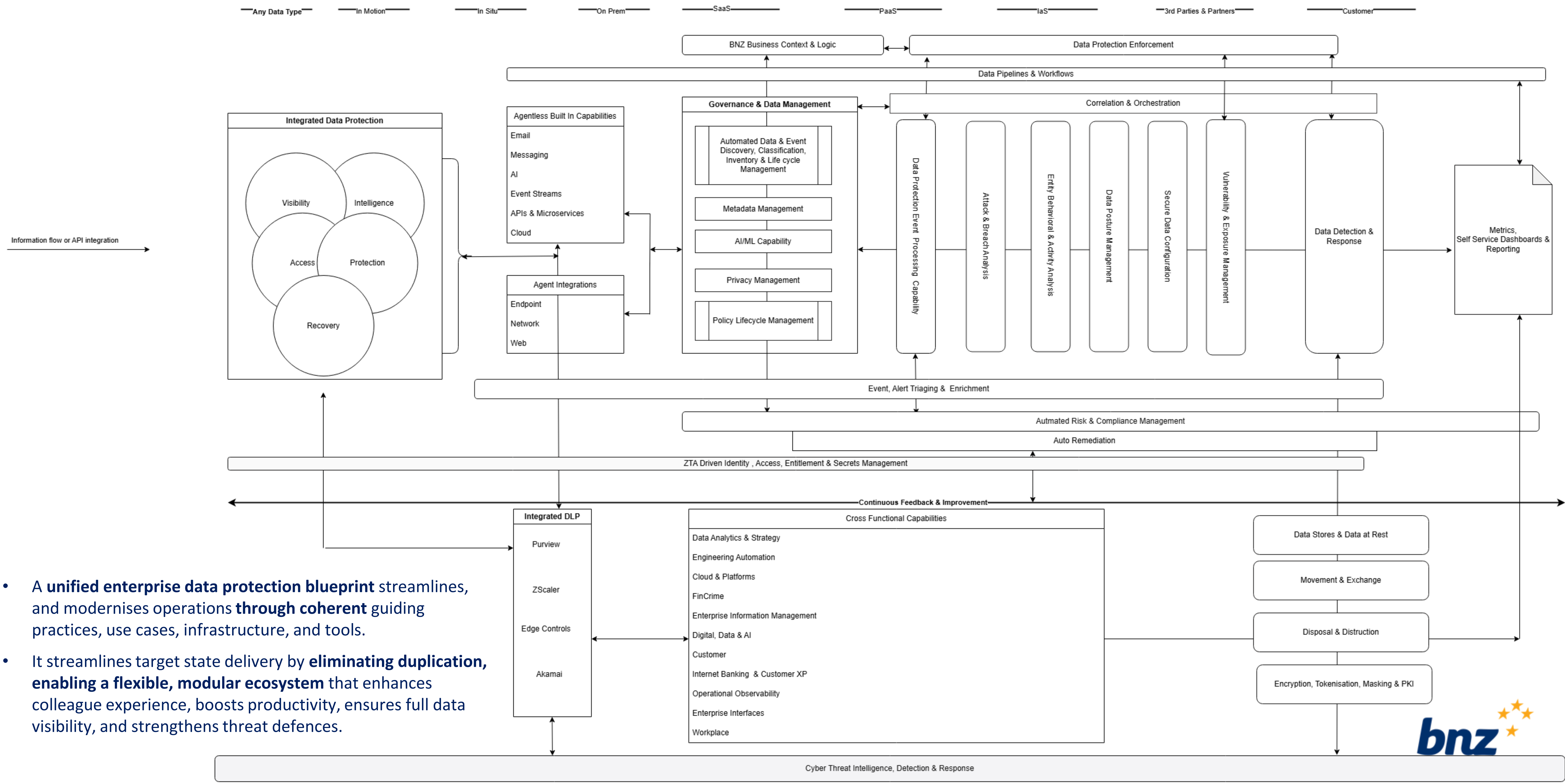
Data Reconciliation

***Party - Prospects, Partners, Regulatory bodies, vendors, etc.** *Note that vendor is called out explicitly here, because the governance of a vendor is different to other parties – per the next slide.*

Data & Information Protection Blueprint

CONFIDENTIAL

This diagram depicts blueprint of how the different components of the ecosystem must mould together to deliver desired ecosystem.



Any Data Type — In Motion — In Situ — On Prem — SaaS — PaaS — IaS — 3rd Parties & Partners — Customer

Information flow or API integration

BNZ Business Context & Logic

Data Protection Enforcement

Data Pipelines & Workflows

Integrated Data Protection

Visibility

Intelligence

Access

Protection

Recovery

Agentless Built In Capabilities

- Email
- Messaging
- AI
- Event Streams
- APIs & Microservices
- Cloud

Agent Integrations

- Endpoint
- Network
- Web

Governance & Data Management

- Automated Data & Event Discovery, Classification, Inventory & Life cycle Management
- Metadata Management
- AI/ML Capability
- Privacy Management
- Policy Lifecycle Management

Correlation & Orchestration

Data Protection Event Processing Capability

Attack & Breach Analysis

Entity Behavioral & Activity Analysis

Data Posture Management

Secure Data Configuration

Vulnerability & Exposure Management

Data Detection & Response

Metrics, Self Service Dashboards & Reporting

Event, Alert Triaging & Enrichment

Autmated Risk & Compliance Management

Auto Remediation

ZTA Driven Identity , Access, Entitlement & Secrets Management

Continuous Feedback & Improvement

Integrated DLP

- Purview
- ZScaler
- Edge Controls
- Akamai

Cross Functional Capabilities

- Data Analytics & Strategy
- Engineering Automation
- Cloud & Platforms
- FinCrime
- Enterprise Information Management
- Digital, Data & AI
- Customer
- Internet Banking & Customer XP
- Operational Observability
- Enterprise Interfaces
- Workplace

Data Stores & Data at Rest

Movement & Exchange

Disposal & Distruction

Encryption, Tokenisation, Masking & PKI

Cyber Threat Intelligence, Detection & Response

- A **unified enterprise data protection blueprint** streamlines, and modernises operations **through coherent** guiding practices, use cases, infrastructure, and tools.
- It streamlines target state delivery by **eliminating duplication, enabling a flexible, modular ecosystem** that enhances colleague experience, boosts productivity, ensures full data visibility, and strengthens threat defences.

SAA Pack

Data & Information Protection Platform Context

The strategy, process and technology for **safe**, **reliable**, **trusted** and **compliant** data and information.

Strategic Drivers

the 'why'

- Customer confidence & trust
- Business continuity & resilience
- Compliance & regulator expectations

Personas

the 'who'

- Customers
- Colleagues
- Party – Prospects, Partners, Regulators, Vendors etc

Governance

the 'what'

- Regulations
- Risk Management
- Policies & Standards
- Controls

Security

the 'how'

- Access Enablement
- Protection
- Detection & Response
- Operational resilience

All data types

Across the whole lifecycle

Everywhere data & information lives and moves

Continuously

Through automation & orchestration

Data & Information Protection Modernisation

From Defence to Confidence: Transforming Data & Information Protection into Enterprise Trust & Resilience

	Cybersecurity-Led	**Technology Enabled**	**Enterprise Trust & Resilience**
	Focused on threat defence, monitoring and incident response	*Embedded protection in platforms & architecture*	*Unified governance, security, and technology with automation, visibility and strategic alignment*
Industry Trends	**Historic** - Rooted in perimeter defence and reactive models; still relevant but evolving	**Transitional** - Supports modern architectures and automation; needs governance integration to mature.	**Future-facing** - Aligns with trends like zero trust, open banking, AI-driven, automated compliance risk, detection and response.
Drivers	Threat landscape, regulatory pressure, need for resilience and proactive breach readiness	Cloud adoption, automation, agile development, platform modernisation.	Hostile Threat landscape, regulatory compliance, digital transformation, **trust and transparency**.
Transition Pathway →			
Key Shifts	- Manual to Automated Controls - Reactive to proactive - Perimeter to identity/data-centric - Siloed to integrated	- Introduces DevSecOps - Automates compliance - Enables real-time monitoring	- Cross-functional ownership - Continuous assurance - Trust and transparency as outcomes - Resilience
Strategic Value	Strong foundation for protection, but limited in agility with digital transformation	Bridges the gap between security and operations; supports scale, agility & cloud first approaches	**Aligns protection with business value and risk appetite. Focussed on enabling and protecting**

Data & Information Protection – BNZ Vision

Enabling BNZ to move faster, operate safer and lead with confidence in a digital first, regulated world.

From Siloed to Orchestrated Governance

- Implement **federated governance** with shared standards and automation tools—empowering platform teams with guardrails, not gates.
- Establish a **Centre of Enablement** to co-ordinate enterprise-wide protection, trust and resilience

From Independent to Collaborative Delivery

- Shift to an **enterprise shared responsibility model**, enabling teams to own protection outcomes with the right support.
- **Equip and incentivise teams** to prioritise secure configuration and data protection outcomes – not just functional delivery.

From Reactive to Proactive Control

- Embed **automated protection** into the **design and deployment lifecycle**—ensuring controls are integrated from the start, not retrofitted.
- Introduce **automated response workflows** to detect and act on anomalies across platforms.

From Tech Uplift to Secure-by-Design

- Leverage existing investment in **cyber**, **cloud transformation** and **data platform modernisation** to embed native protection capabilities.
- Make data protection a **default part of platform engineering**, not an afterthought.

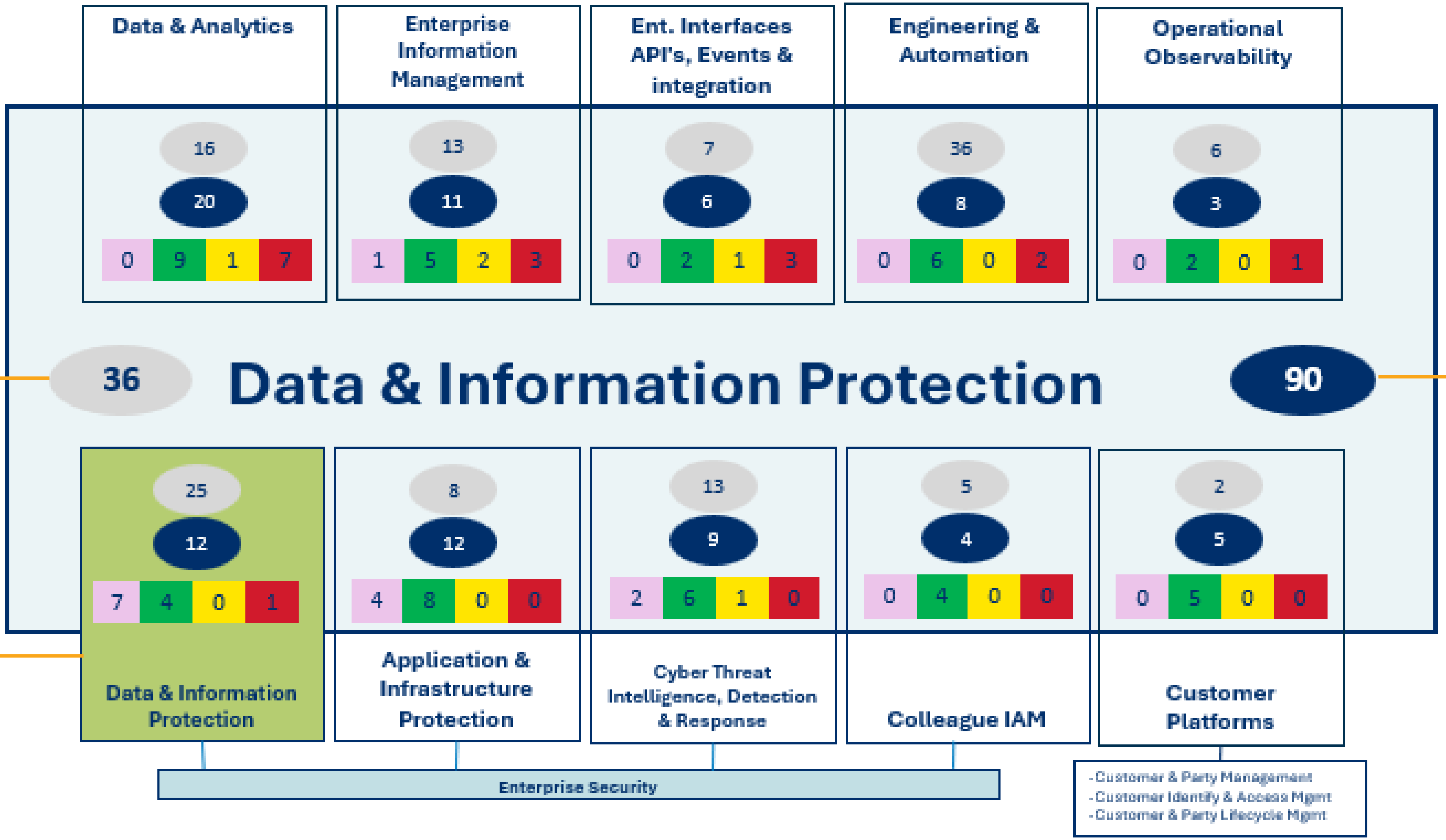
From Cyber-centric to Enterprise Enablement

- Build a **policy translation layer** to convert business protection needs into scalable, platform-specific enforcement.
- Enable **cross-platform visibility and orchestration** to align protection with enterprise priorities and delivery pipelines.

Current State Overview

Data & Information Protection capability coverage is achieved across **many platforms & technologies.**

36 capabilities in Data & Information Protection



36 Data & Information Protection 90

Data & Analytics	16	20	0	9	1	7
Enterprise Information Management	13	11	1	5	2	3
Ent. Interfaces API's, Events & integration	7	6	0	2	1	3
Engineering & Automation	36	8	0	6	0	2
Operational Observability	6	3	0	2	0	1
Data & Information Protection	25	12	7	4	0	1
Application & Infrastructure Protection	8	12	4	8	0	0
Cyber Threat Intelligence, Detection & Response	13	9	2	6	1	0
Colleague IAM	5	4	0	4	0	0
Customer Platforms	2	5	0	5	0	0

Enterprise Security

- Customer & Party Management
- Customer Identify & Access Mgmt
- Customer & Party Lifecycle Mgmt

90+ technologies across the capabilities

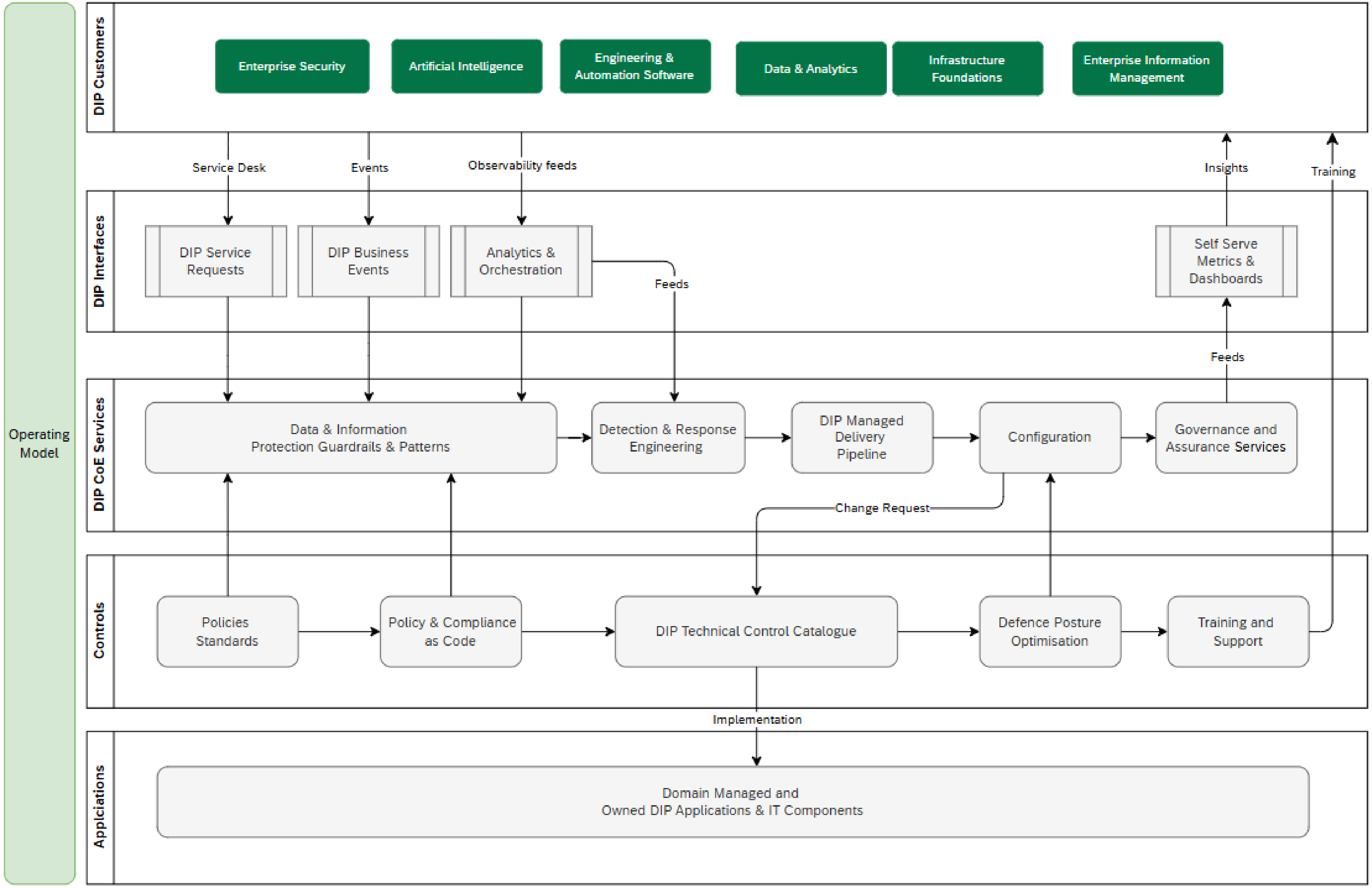
There are more!

The **platform as it is represented today** does not cover Data & Information Protection at BNZ

Current State Challenges

- **Fragmented and inconsistent protection** – Data protection efforts are not co-ordinated, making it hard to know what is protected across the ecosystem.
- **Legacy systems and limited capability** – Outdated technologies and complex data flows hinder our ability to protect data effectively.
- **Disparate standards and guidance** – There is no unified approach across cyber, tech, and governance, leaving teams without clear direction
- **Reactive rather than proactive** – We often respond to issues after they occur, with limited tools to detect and prevent risks early.
- **Compliance and change challenges** – We retain more data than needed, struggle to meet compliance confidently, and face resistance when improving protection.

Target State - Conceptual


Operating Model
DIP Customers
Enterprise Security
Artificial Intelligence
Engineering & Automation Software
Data & Analytics
Infrastructure Foundations
Enterprise Information Management
Service Desk
Events
Observability feeds
Insights
Training
DIP Interfaces
DIP Service Requests
DIP Business Events
Analytics & Orchestration
Feeds
Self Serve Metrics & Dashboards
Feeds
DIP CoE Services
Data & Information Protection Guardrails & Patterns
Detection & Response Engineering
DIP Managed Delivery Pipeline
Configuration
Governance and Assurance Services
Change Request
Controls
Policies Standards
Policy & Compliance as Code
DIP Technical Control Catalogue
Defence Posture Optimisation
Training and Support
Implementation
Applciations
Domain Managed and Owned DIP Applications & IT Components

Customer Layer: Platform owners who, through training and insights, can access DIP services via the interface layer.

Interface Layer: Defining how to engage data and information protection platform support and delivery services.

CoE Services Layer: Defines the services available, from prepared patterns, guardrails, to the delivery of configuration changes, recommendations and insights

DIP Control Layer: Catalogue of governed risk mitigations, including policies, standards, training and support.

Application Support Layer: representing the technologies responsible for implementing the configuration changes

Data & Information Protection - Key Messages Recap

Enabling BNZ to move faster, operate safer and lead with confidence in a digital first, regulated world.

Leadership commitment drives success

- Long-term value in Data & Information Protection comes from sustained leadership, smart investment and visible sponsorship

Enterprise Shared Responsibility

- Beyond cyber – everyone plays a role. Data Protection spans strategy, tech, and operations – wherever data lives and moves

Drivers for change

- Proactive, data-centric protection replaces reactive cybersecurity.
- End-to-end observability enables smarter compliance and threat response
- Co-ordinated execution delivers scalable, consistent outcomes

Five Platform Transformations

From	To
Siloed	Orchestrated Governance
Independent	Collaborative Delivery
Reactive	Automated & Proactive controls
Technology-led platform uplift	Secure-by-design
Cyber-centric	Enterprise-aligned

Exec Pack

Data & Information Protection

The strategy, process, technology and practice for safe, reliable, trusted and compliant data and information.

The target state enables BNZ to move faster, operate safer and lead with confidence in a digital first, regulated world.

Re-use the capabilities in existing technologies across platforms to uplift Data & Information Protection capability across the enterprise

Define and communicate **standards, patterns & tools** for the enterprise to ensure consistent protection practices and streamline compliance

Apply **DataSecOps** to embed automated Data & Information protection continuously across the lifecycle to ensure protection is built-in rather than added as an afterthought.

Introduce Data & Information Protection **Observability** across the enterprise to gain real-time visibility into sensitive data usage, threat detection and compliance

Introduce **Automation** in detection & response, to rapidly identify and mitigate threats while reducing manual effort and response time.

Look for **efficiency gains in AI** that can improve Data & Information Protection

Scope & Context

Effective Data & Information Protection requires deep integration with where data lives and moves – across the entire technology ecosystem, not within the boundaries of any single platform.

Transformation Approach

An evolution from reactive, siloed cybersecurity practices to a unified model that embeds governance, security, and technology across platforms and teams. Using a technology enabled phase as a bridge, to build the operational maturity needed to achieve enterprise-wide trust, resilience and agility.

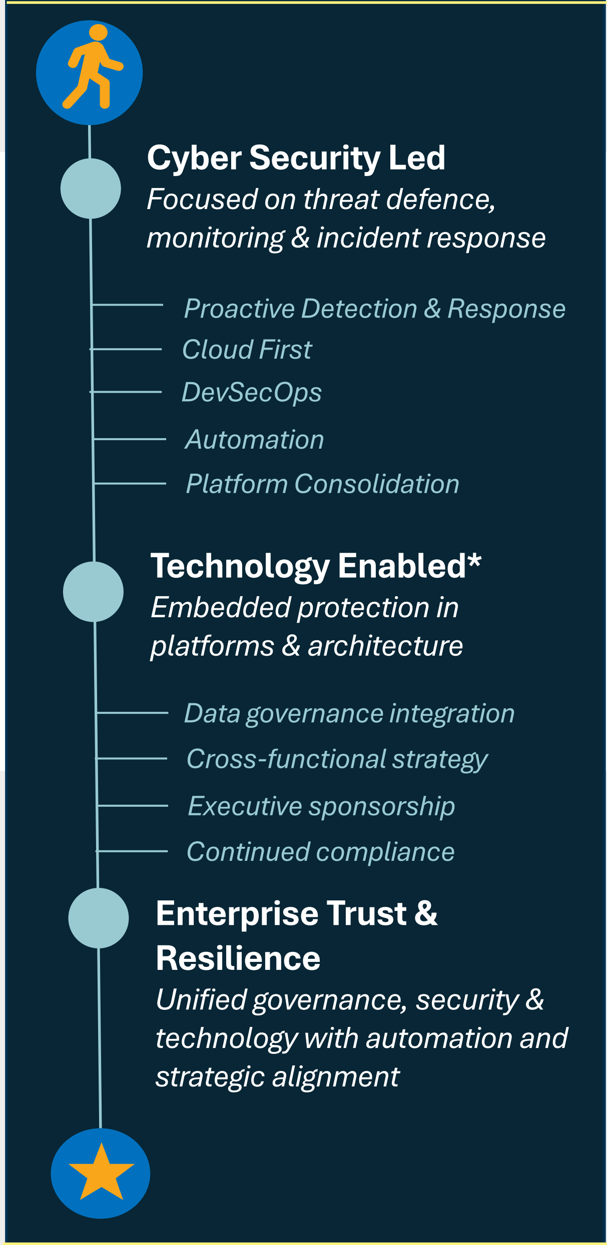
Current State - BMI View

BMI is represented in technologies across other platforms in BNZ, rather than in Data & Information Protection itself.

NAB Alignment

NAB haven't adopted Data & Information Protection as a platform, however the approach is similar in building protection with capabilities from other platforms. BNZ & NAB are targeting similar outcomes across contributing platforms e.g. secure-by-design, proactive risk and threat informed protection.

Modernisation Roadmap



Cyber Security Led
Focused on threat defence, monitoring & incident response

- *Proactive Detection & Response*
- *Cloud First*
- *DevSecOps*
- *Automation*
- *Platform Consolidation*

Technology Enabled*
Embedded protection in platforms & architecture

- *Data governance integration*
- *Cross-functional strategy*
- *Executive sponsorship*
- *Continued compliance*

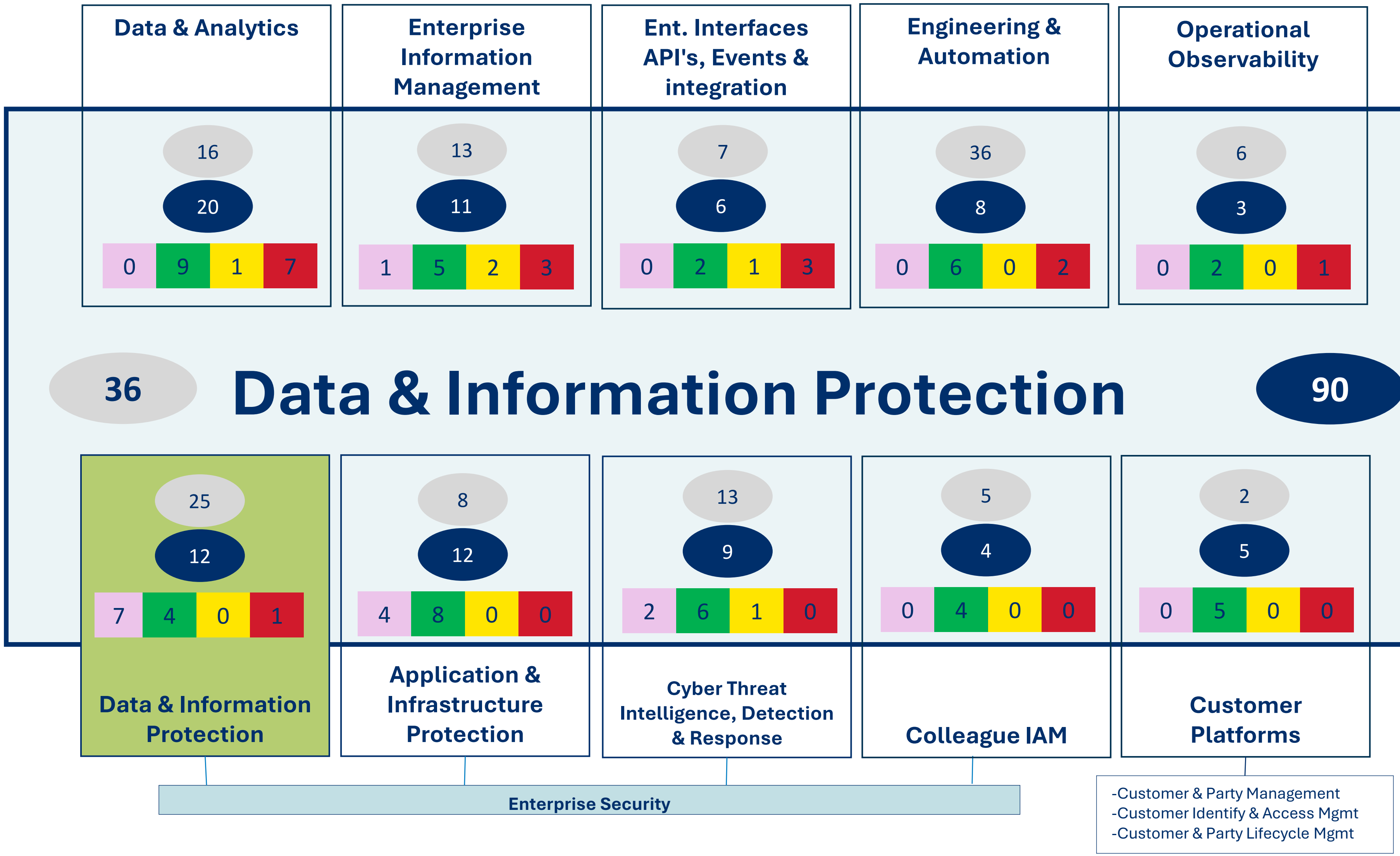
Enterprise Trust & Resilience
Unified governance, security & technology with automation and strategic alignment

** Technology Enabled - some work in this phase already*

Current State – Broader view

Note – *there are more technologies & platforms*

In protecting data and information across the entire ecosystem, there are many technologies that contribute to Data & Information Protection.



Data & Information Protection

	# DIP Capabilities	# Technologies	Innovate	Encourage	Contain	Exit
Data & Information Protection	36	90				
Data & Analytics	16	20	0	9	1	7
Enterprise Information Management	13	11	1	5	2	3
Ent. Interfaces API's, Events & integration	7	6	0	2	1	3
Engineering & Automation	36	8	0	6	0	2
Operational Observability	6	3	0	2	0	1
Data & Information Protection	25	12	7	4	0	1
Application & Infrastructure Protection	8	12	4	8	0	0
Cyber Threat Intelligence, Detection & Response	13	9	2	6	1	0
Colleague IAM	5	4	0	4	0	0
Customer Platforms	2	5	0	5	0	0

Enterprise Security

-Customer & Party Management
-Customer Identify & Access Mgmt
-Customer & Party Lifecycle Mgmt

Technology Lifecycle Status Key

- Innovate
- Encourage
- Contain
- Exit
- # DIP Capabilities
- # Technologies

Challenges & Issues

- **Fragmented and inconsistent protection** – Data protection efforts are not co-ordinated, making it hard to know what is protected across the ecosystem.

- **Legacy systems and limited capability** – Outdated technologies and complex data flows hinder our ability to protect data effectively.

- **Fragmented standards and guidance** – There's no unified approach across cyber, tech, and governance, leaving teams without clear direction

- **Reactive rather than proactive** – We often respond to issues after they occur, with limited tools to detect and prevent risks early.

- **Compliance and change challenges** – We retain more data than needed, struggle to meet compliance confidently, and face resistance when improving protection.

Recap - Key Messages

Enabling BNZ to move faster, operate safer and lead with confidence in a digital first, regulated world

Leadership commitment is essential for success

- Achieving this requires executive buy-in, sustained commitment, and targeted investment to drive meaningful change and deliver long-term value.

Data & Information Protection is an enterprise shared responsibility

- For delivering the strategy, process, technology and practice for safe, reliable, trusted and compliant data and information.
- Across many technologies & platforms – wherever data is being used, lives and moves.
- Thus going **beyond being seen as a cyber only responsibility**.

Drivers for change

- **Evolution toward proactive, data-centric protection** that addresses broader information risks and obligations. The current Cybersecurity focus is effective, but reactive with limited agility.
- **End-to-end observability** is essential to understand how we meet compliance obligations, identify gaps, detect threats, and target uplift where it delivers the greatest value.
- **Co-ordinated execution** is key to achieving consistent, scalable outcomes. Fragmented delivery across technologies and teams limits effectiveness.

Transformation

- Siloed to **Orchestrated Governance and Assurance**
- Blind spots to **continuous visibility**
- Independent to **Collaborative Delivery**
- Reactive to **Automated & Proactive Controls**
- Utilising existing **investment in technology and programmes** (where possible).
- Cyber centric to **Enterprise Alignment through a shared responsibility operating model.**

Data & Information Protection Modernisation

From Defence to Confidence: Transforming Data & Information Protection into Enterprise Trust & Resilience

	Cybersecurity-Led *Focused on threat defence, monitoring and incident response*	**Technology Enabled** *Embedded protection in platforms & architecture*	**Enterprise Trust & Resilience** *Unified governance, security, and technology with automation, visibility and strategic alignment*
Industry Trends	**Historic** - Rooted in perimeter defence and reactive models; still relevant but evolving	**Transitional** - Supports modern architectures and automation; needs governance integration to mature.	**Future-facing** - Aligns with trends like zero trust, open banking, AI-driven, automated compliance risk, detection and response.
Drivers	Threat landscape, regulatory pressure, need for resilience and proactive breach readiness	Cloud adoption, automation, agile development, platform modernisation.	Hostile Threat landscape, regulatory compliance, digital transformation, **trust and transparency**.
Transition Pathway →			
Key Shifts	- Manual to Automated Controls - Reactive to proactive - Perimeter to identity/data-centric - Siloed to integrated	- Introduces DevSecOps - Automates compliance - Enables real-time monitoring	- Cross-functional ownership - Continuous assurance - Trust and transparency as outcomes - Resilience
Strategic Value	Strong foundation for protection, but limited in agility with digital transformation	Bridges the gap between security and operations; supports scale, agility & cloud first approaches	**Aligns protection with business value and risk appetite. Focussed on enabling and protecting**

Data & Information Protection – BNZ Vision

Enabling BNZ to move faster, operate safer and lead with confidence in a digital first, regulated world.

From Siloed to Orchestrated Governance

- Implement **federated governance** with shared standards and automation tools—empowering platform teams with guardrails, not gates.
- Establish a **Centre of Enablement** to co-ordinate enterprise-wide protection, trust and resilience

From Independent to Collaborative Delivery

- Shift to an **enterprise shared responsibility model**, enabling teams to own protection outcomes with the right support.
- **Equip and incentivise teams** to prioritise secure configuration and data protection outcomes – not just functional delivery.

From Reactive to Proactive Control

- Embed **automated protection** into the **design and deployment lifecycle**—ensuring controls are integrated from the start, not retrofitted.
- Introduce **automated response workflows** to detect and act on anomalies across platforms.

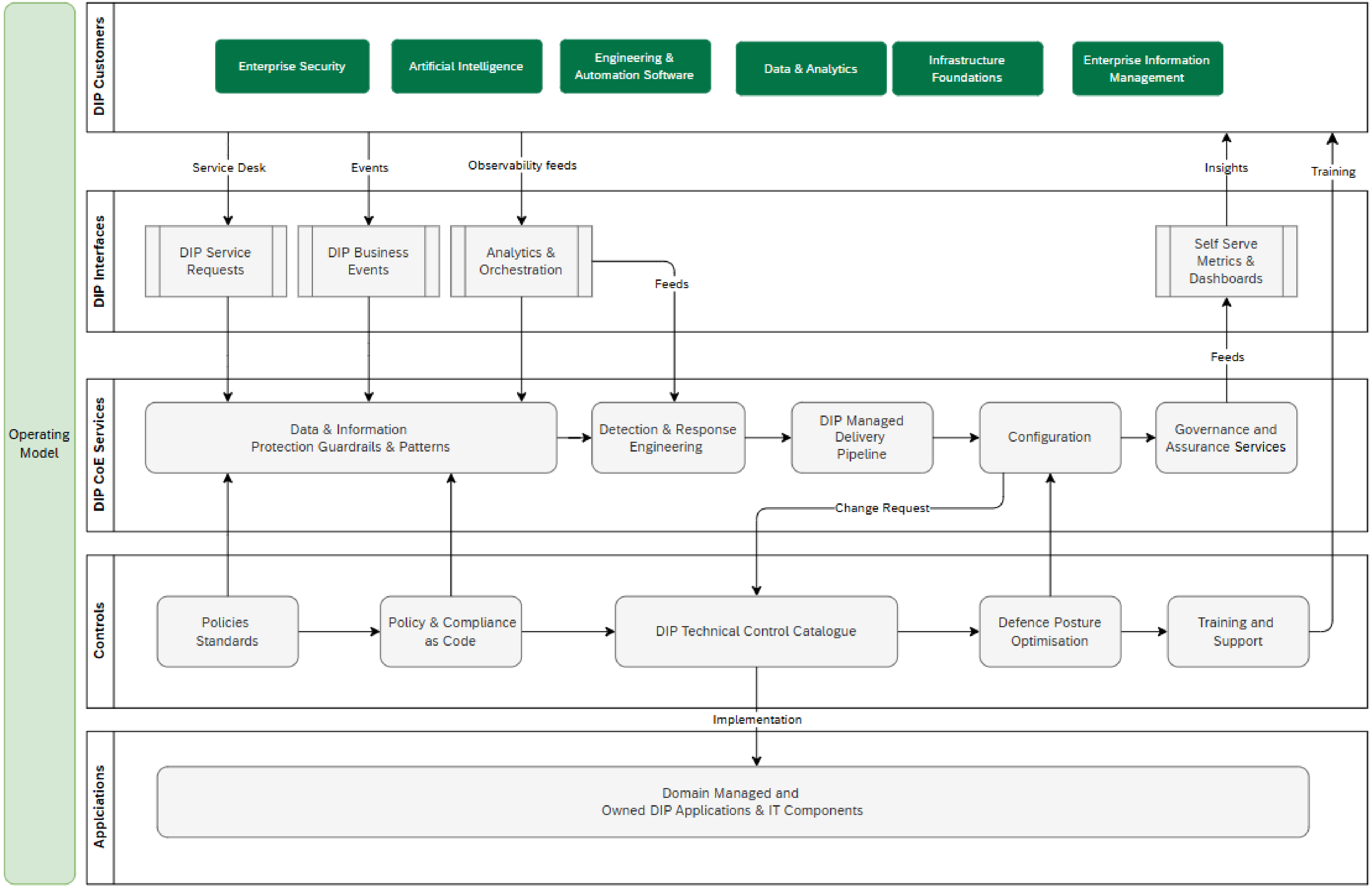
From Tech Uplift to Secure-by-Design

- Leverage existing investment in **cyber**, **cloud transformation** and **data platform modernisation** to embed native protection capabilities.
- Make data protection a **default part of platform engineering**, not an afterthought.

From Cyber-centric to Enterprise Enablement

- Build a **policy translation layer** to convert business protection needs into scalable, platform-specific enforcement.
- Enable **cross-platform visibility and orchestration** to align protection with enterprise priorities and delivery pipelines.

Target State - Conceptual


Operating Model
DIP Customers
Enterprise Security
Artificial Intelligence
Engineering & Automation Software
Data & Analytics
Infrastructure Foundations
Enterprise Information Management
Service Desk
Events
Observability feeds
Insights
Training
DIP Interfaces
DIP Service Requests
DIP Business Events
Analytics & Orchestration
Feeds
Self Serve Metrics & Dashboards
Feeds
DIP CoE Services
Data & Information Protection Guardrails & Patterns
Detection & Response Engineering
DIP Managed Delivery Pipeline
Configuration
Governance and Assurance Services
Change Request
Controls
Policies Standards
Policy & Compliance as Code
DIP Technical Control Catalogue
Defence Posture Optimisation
Training and Support
Implementation
Applciations
Domain Managed and Owned DIP Applications & IT Components

Customer Layer: Platform owners who, through training and insights, can access DIP services via the interface layer.

Interface Layer: Defining how to engage data and information protection platform support and delivery services.

CoE Services Layer: Defines the services available, from prepared patterns, guardrails, to the delivery of configuration changes, recommendations and insights

DIP Control Layer: Catalogue of governed risk mitigations, including policies, standards, training and support.

Application Support Layer: representing the technologies responsible for implementing the configuration changes

Feedback Themes

In sharing in more detail with GMs and DD&A teams, feedback is showing up in these areas:

- **Yes!** – **Enterprise trust and resilience** is what we want to be targeting for BNZ, it is the right approach.

- It is great direction and **very ambitious**, how do we break it down and roadmap the journey so it is achievable? Keep in mind the practicalities of achieving it.

- Leadership involvement – how will the **shared accountability** show up practically? We see challenges in that today, where an issue pops up we need to make sure that the accountability is clear

- **Centre of Enablement -** Practically, where would CoE sit? Who would be the key areas that need to be involved. And, should it be called Centre of Enablement, or something else?

- The **balance** between the need to protect and the need to enable is important, we must get that right.

- While we don't have CoE now, **how do we solve for gaps** like synthetic test data, with an enterprise approach **in the meantime**?

bnz