



SAM FARIBORZ
JULY 2024



BUILDING A CYBERSECURITY PROGRAM

Business & Tech Drivers

- Corporate Strategy
- Technology Strategy
- Previous Audit Reports

Regulations & Industry Drivers

- Critical Infrastructure
- Payment Card Industry Data Security Standard
- Etc.

Information Gathering

- Tech Stakeholders
- Business Stakeholders



Our Mission Is:

To Provide practical and enabling cyber services that advise upon and manage security risk.

What We Will Achieve:

Prevent undesirable business impact from cyber risks, manifesting to enable growth via secure digital investments and enhance customer relationships and data through improved trust and royalty.





Level 1- Initial	Level 2- Managed	Level 3- Defined	Level 4- Enhanced	Level 5- Optimised
Controls do not exist or are largely ad-hoc, there are a material number of implementation gaps or control deficiencies.	Controls exist and are mostly formalized, there are a manageable number of implementation gaps or control deficiencies.	Controls are formalized, there are a few implementation gaps or control deficiencies, and metrics are defined but not always measured.	Controls are enhanced taking into consideration the business context (inc. risk appetite). Metrics are measured, reported on and are used to maintain and increase the performance of the capability. Processes demonstrate sustainability, continues improvement and refinement.	Controls are advanced and often rely on bespoke or highly optimized tooling that goes beyond what is available commercially. Regular cycles of improvement are applied based on a continuous improvement program.
Identify (ID)	X	Emerging processes are in place for some key areas, such as risk management and 3rd party assessments, Beyond these elements there are numerous areas with extremely limited maturity or coverage, including		
Protect (PR)	X	Some baseline capabilities are in place, for example, but even there is significant		
Detect (DE)	X	David Jones' detection capability has Further analysis is also required to determine the level of business context incorporated into		
Respond (RS)	X	As with Detect, maturity in some areas of Respond and Recover are Notable gaps in this space include....		
Recover (RC)	X			
Average self-assessment	X			
Average industry benchmark	X			

NIST Assessment Significant Gaps

Identify	Governance	<ul style="list-style-type: none">• X• Y
	Identity and Access Management	<ul style="list-style-type: none">• X• Y
Protect	Awareness and Training	<ul style="list-style-type: none">• X• Y
	Security Detection and Continuous Monitoring	<ul style="list-style-type: none">• X• Y
Detect		
Respond	Vulnerabilities Mitigation	<ul style="list-style-type: none">• X• Y

Cyber Program Streams

Security Governance

- Establish an effective cyber security practice within the business

Identity and Access Management

- Establish an effective identity management capability to support user and system identities

Security Awareness and Culture

- Provide effective cyber security training and guidance to all employees

Threat and Vulnerability Management

- Ensure that threats are identified, and vulnerabilities are proactively managed

Security Incidents Detection, Continuous Monitoring and Response

- Ensure readiness for timely and effective responses to security and other major incidents
- Monitor and correlate security events of interest enabling rapid detection of security events

Future maturity uplift

Targeted maturity increase and continual improvement once baseline control maturity is sufficient.

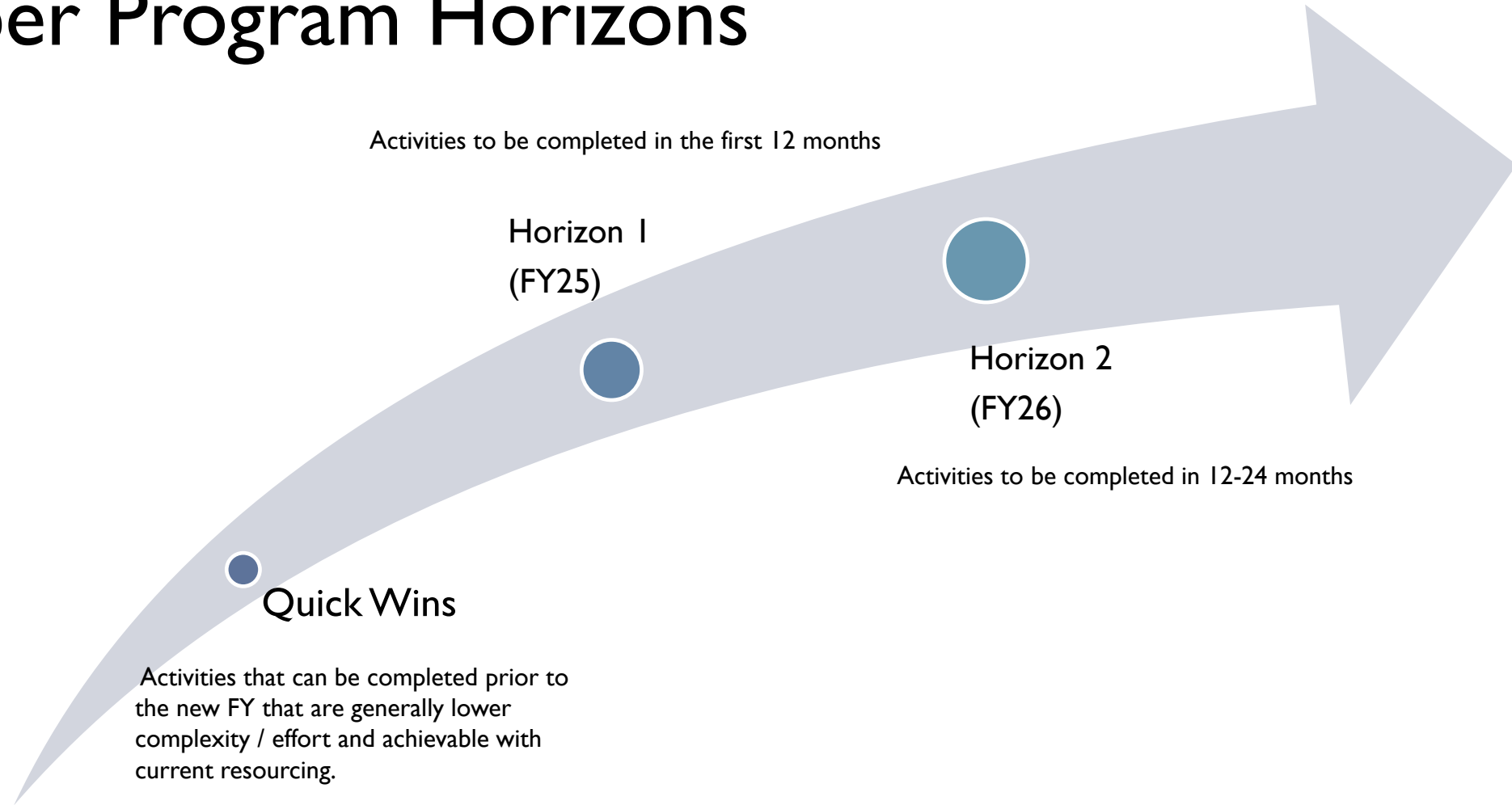
Execution by other areas

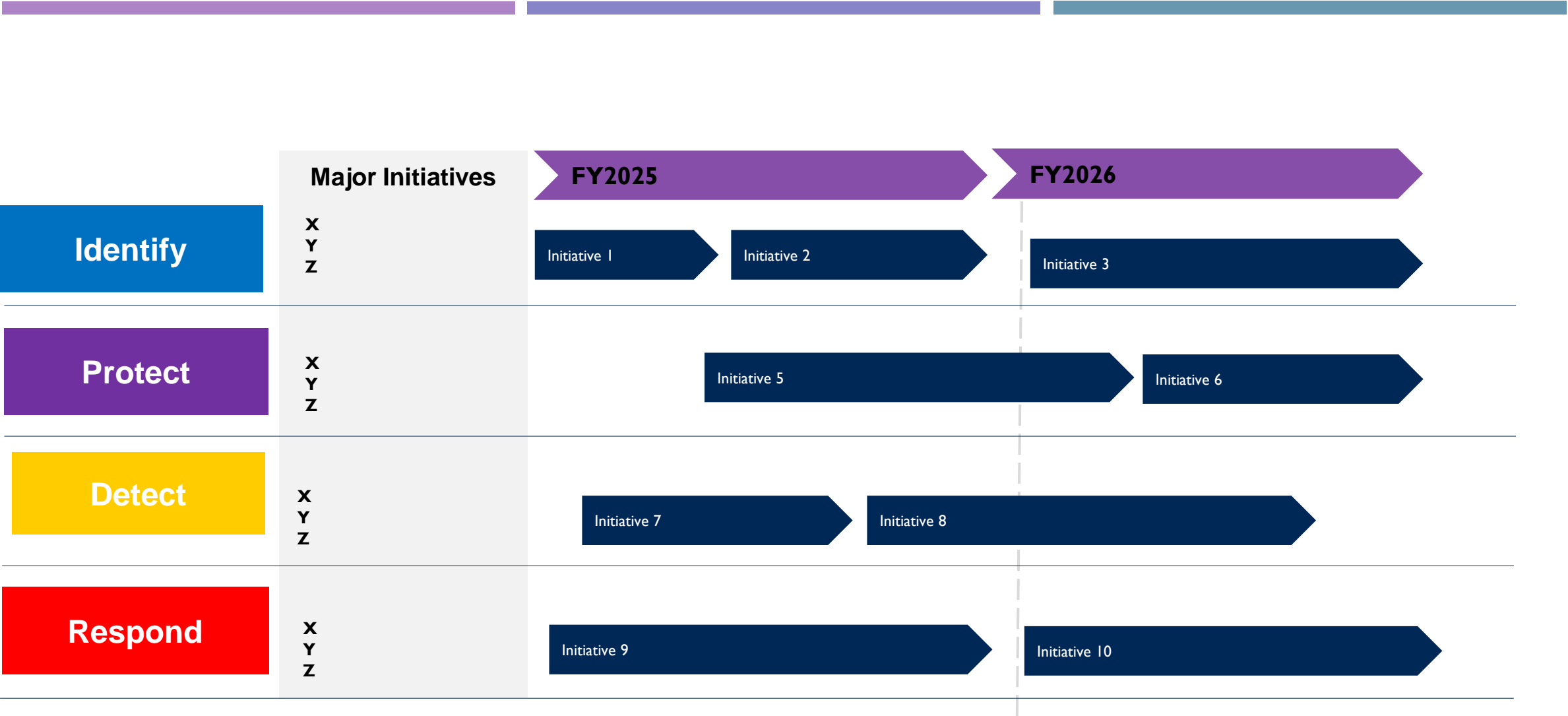
Elements of security incorporated into other streams of work adhering to revised principles, policies, standards, target state architecture and governance


CYBER SECURITY PROGRAM APPROACH

<i>Shaping new initiatives and changes</i>	<i>Remediation of existing assets</i>	<i>Security specific initiatives and activities</i>
<ul style="list-style-type: none">• <i>Cyber security principles</i>• <i>Security solution architecture process</i>• <i>Security risk management</i>• <i>Vendor assessment process</i>	<ul style="list-style-type: none">• <i>Where significant gaps exist in core platforms</i>	<ul style="list-style-type: none">• <i>Establishment and roll-out of core security capabilities</i>
<p>The funding of security elements of new initiatives and changes will be part of the initiative or change costing.</p>	<p>The funding mechanism for these may be either incorporate into the security program or completed by each platform.</p>	<p>These activities will be funded and managed independently of other projects or activities.</p>

Cyber Program Horizons





- 
- Leadership endorsement and support
 - Managing dependencies to other programs and teams
 - Alignment with the PMO/WoW

Identity and Access Management

Protect

Identity Management
Awareness and Training
Data Security
Information Protection Processes & Procedures
Maintenance
Protective Technology

Key Initiatives

- Develop and socialise non-customer identity management strategy.
- IDP clean up.
- Develop and socialise customer identity management strategy.
- Determine identity management tooling / licensing.
- Complete review of all existing systems for identity integration status.
- Develop roadmap for identity integration for existing systems.

Key Outcomes

- Only active users with a demonstrated requirement for access are present in IDP.
- SSO is enforced for all systems
- Provisioning and de-provisioning is automated for all users, including for user entitlements.
- User self-service is available for requesting and managing most access.
- Automated user access reviews are being completed, with access being automatically removed if no longer required.
- Least privilege is effectively applied.

Key Metrics

- X
- Y
- Z

Initiative Name

Initiative leader:....

Cyber Program Stream

Overview



Status & Progress – On-track
Change Variation – No change variation

Management Action No

Finance	Risk	Schedule	Overall
<div></div>	<div></div>	<div></div>	<div></div>

Key Achievements Last Month

Next Month Planned Activities

S. No.	Milestone	Status	Due Date
01	Discovery	In Progress	
02	Gap Assessment	In Progress	TBC
03			
04			

Risk ID	Risk Description	Impact	Mitigation Plan	Owner	Status
01					
02					

Issue ID	Issue Description	Impact	Mitigation Plan	Owner	Status
----------	-------------------	--------	-----------------	-------	--------



THANK YOU