Cybersecurity Risk Management Program
2024

Findings and Recommendations

September 5th, 2024

Our Agenda

- Risk Assessment Overview
- Key Findings
- Key Recommendations
- Measuring Risk Management

Risk Assessment Overview: Timeline

Step	Start Date	End Date	Status
Information gathering	12 Mar 24	23 Apr 24	Complete
Defined risk assessment criteria	09 May 24	09 May 24	Complete
Risk analysis and reporting	09 May 24	24 Jun 24	Complete
Risk management roadmap	12 Jul 24	29 Jul 24	Complete

Scope:	IT Systems and Operations

Risk Assessment Overview: Methods

Maturity Assessment Evaluating the strength of our controls and how they compare to peers.

Helpful quote: “How comprehensively have we implemented our controls?”

Risk Assessment Estimating the likelihood of security events and their impacts.

Helpful quote: “What is the likelihood that ‘x’ will create a problem, and how bad can it hurt?”

Duty of Care Risk Analysis Using safeguards that are no more burdensome to us than risks are to others.

Helpful quote: “The cure cannot be worse than the illness.”

HIT Index HALOCK’s data about the commonality of causes of incidents in each industry.

Helpful quote: “How do we compare to our similar organizations who were breached?”

Risk Assessment Criteria

Impact definitions	***Mission***	***Objectives***	***Obligations***
	Empower members to find financial freedom and to be the most personal, trusted, and valued source of financial well-being.	*Consistently and effectively meeting operation, capital earning, and customer satisfaction goals.*	*Duty of Care to safeguard members and employees. Compliance to contractual and board agreements, PCI-DSS, State, GDPR, CCPA, and NCUA requirements.*
1. Negligible	No impact to mission.	Goals are on target with no negative impacts.	Exposed PII is under reporting threshold (<100 records). No regulatory or agreement violations.
2. Acceptable	Any impact to mission would be within planned variance.	Slight negative impact, but goals are on target within planned variance.	Exposed sensitive information would not cause foreseeable harm and less than 1,000 records. Regulatory and agreement violations are mitigated with compensating controls.
3. Unacceptable	Impact to mission would take six months to recover.	Impact adversely affects meeting goals and requires effort to recover within a fiscal year.	Over 1,000 PII records were exposed, or information could cause harm a few victims. Control is in violation of regulations or agreements.
4. High	Impact to mission would take 1-2 years to recover.	Significant impact hinders meeting goals and requires multiple years to recover.	Over 100,000 PII records were exposed or leaked information caused harm to many victims. Control could cause fines or a breach of contract due to non-compliance.
5. Catastrophic	Impact to mission would take over 2 years to recover.	Business operations, capital earnings, and customer satisfaction goals are unable to recover.	Members or employees are in constant jeopardy due to data breaches. Non-compliant critical controls led to breach of contract and/or heavy fines.

Risk Assessment: Threat Clusters

Personnel Error A personnel error issue means identifying a threat or security incident that originates from human error or mistakes made by individuals within the organization.

Hacking System A hacking system threat refers to identifying a threat that arises from external actors attempting to gain unauthorized access to the organization's systems or networks.

Hacking Web A hacking web threat specifically focuses on threats that target web-based systems, applications, or websites.

Malware A malware threat involves threats posed by malicious software or code designed to compromise systems, steal data, or disrupt operations.

Personnel Misuse Personnel misuse refers to identifying threats originating from individuals intentionally misusing their access privileges or abusing their authorized access to systems or data.

Risk Assessment: Threat Clusters

Social Engineering
A social engineering threat refers to threats that exploit human psychology or manipulation to deceive individuals and gain unauthorized access to systems or sensitive information.

Physical Facility
A physical facility threat involves threats that target the organization's physical premises, such as offices, data centers, or warehouses.

Physical Loss
Physical loss threats involve risks associated with the loss or damage of physical assets, such as hardware devices, storage media, or documents containing sensitive information.

Point of Sale
Threats that directly target the POS system itself, including the hardware, software, and associated infrastructure.

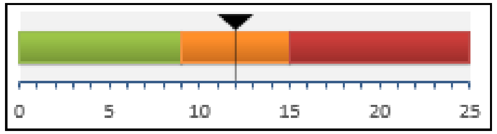
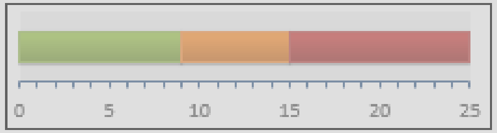
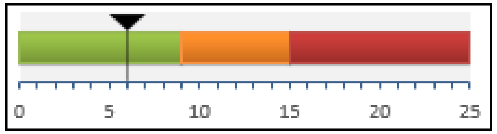
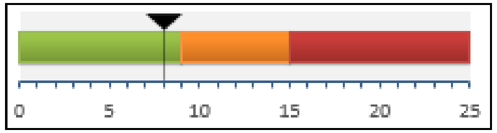
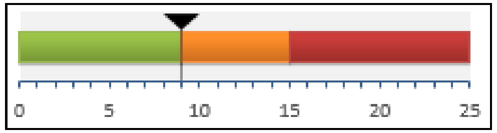
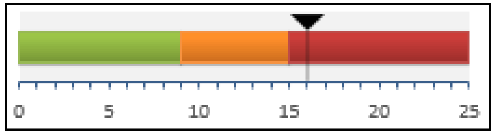
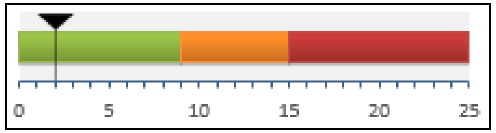
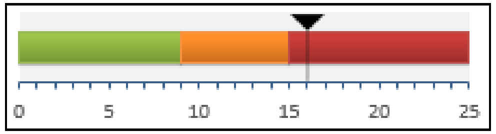
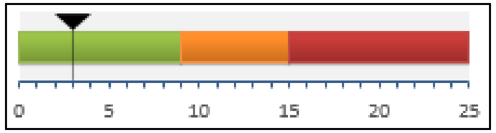
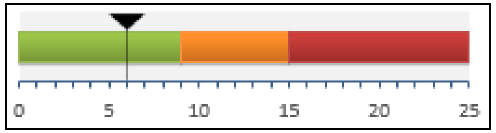
What Threats are Most Commonly Harming Similar Organizations?

Order	Threat Cluster	Occurrence
1	Physical Facility	53%
2	POS	44%
3	Physical Asset Loss	40%
4	Personnel Error	32%
5	Personnel Misuse	25%
6	Hacking System	21%
7	Social Engineering	12%
8	Hacking Web	7%
9	Malware	6%
10	System Failure	0%

How Mature are Our Security Controls?

Order	Threat Cluster	Maturity of Preventive Controls
1	Physical Facility	4.2 out of 5
2	POS	Not Assessed
3	Physical Asset Loss	4 out of 5
4	Personnel Error	4 out of 5
5	Personnel Misuse	3.9 out of 5
6	Hacking System	3.8 out of 5
7	Social Engineering	4 out of 5
8	Hacking Web	3.6 out of 5
9	Malware	4.6 out of 5
10	System Failure	3.7 out of 5

How Do Our Risks Compare to Similar Organizations Who Were Breached?

Order	Threat Cluster	Occurrence	Your Associated Risk
1	Physical Facility	53%	
2	POS	44%	
3	Physical Asset Loss	40%	
4	Personnel Error	32%	
5	Personnel Misuse	25%	
6	Hacking System	21%	
7	Social Engineering	12%	
8	Hacking Web	7%	
9	Malware	6%	
10	System Failure	0%	

HALOCK®

Strong Foundations and Practices

Asset Management

Why this is important Excels in asset management with formal processes, regular audits, and robust security controls, ensuring comprehensive protection of assets against unauthorized access and threats.

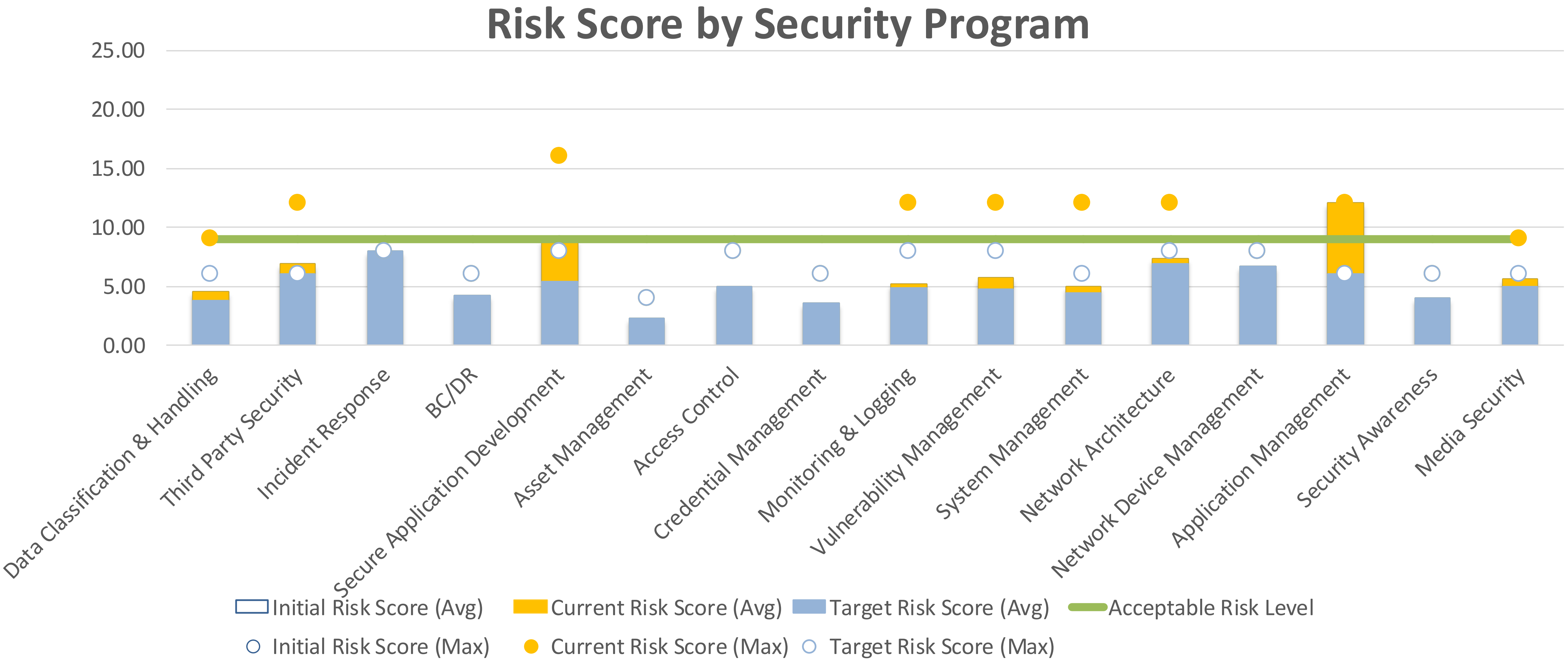
Access Control and Credential Management

Why this is important Enforces strong access control and credential management with RBAC, centralized processes via SailPoint and Delinea, ensuring secure, role-based access and regular credential rotation.

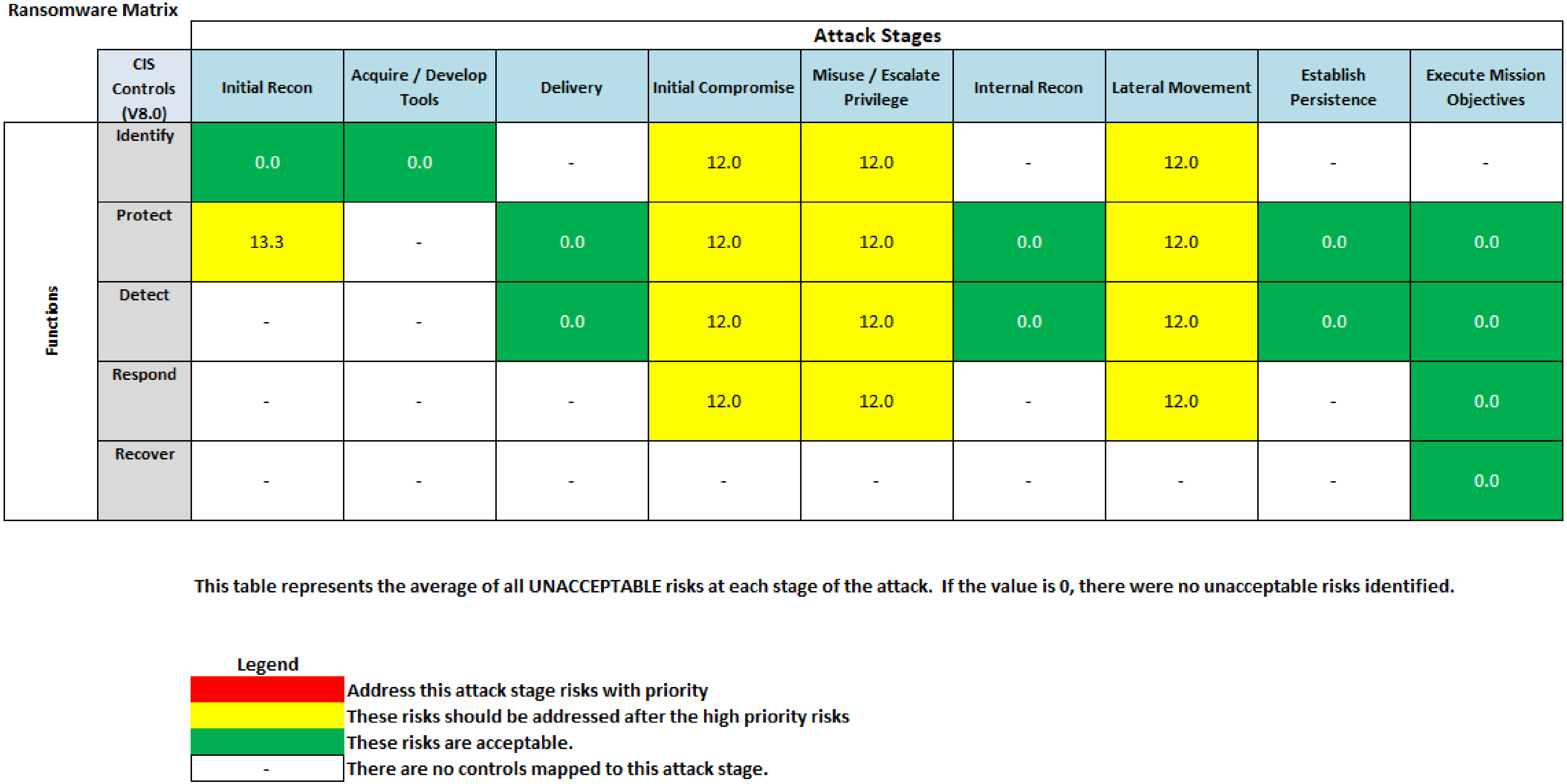
Incident Response and Business Continuity / Disaster Recovery

Why this is important Incident Response and BC/DR plans are well-established, with annual tests, detailed roles, escalation procedures, and cloud-backed recovery systems ensuring resilience against disruptions.

How Controls Are Associated with Risks



MITRE ATT&CK Mapping – Ransomware Matrix



Ransomware Matrix

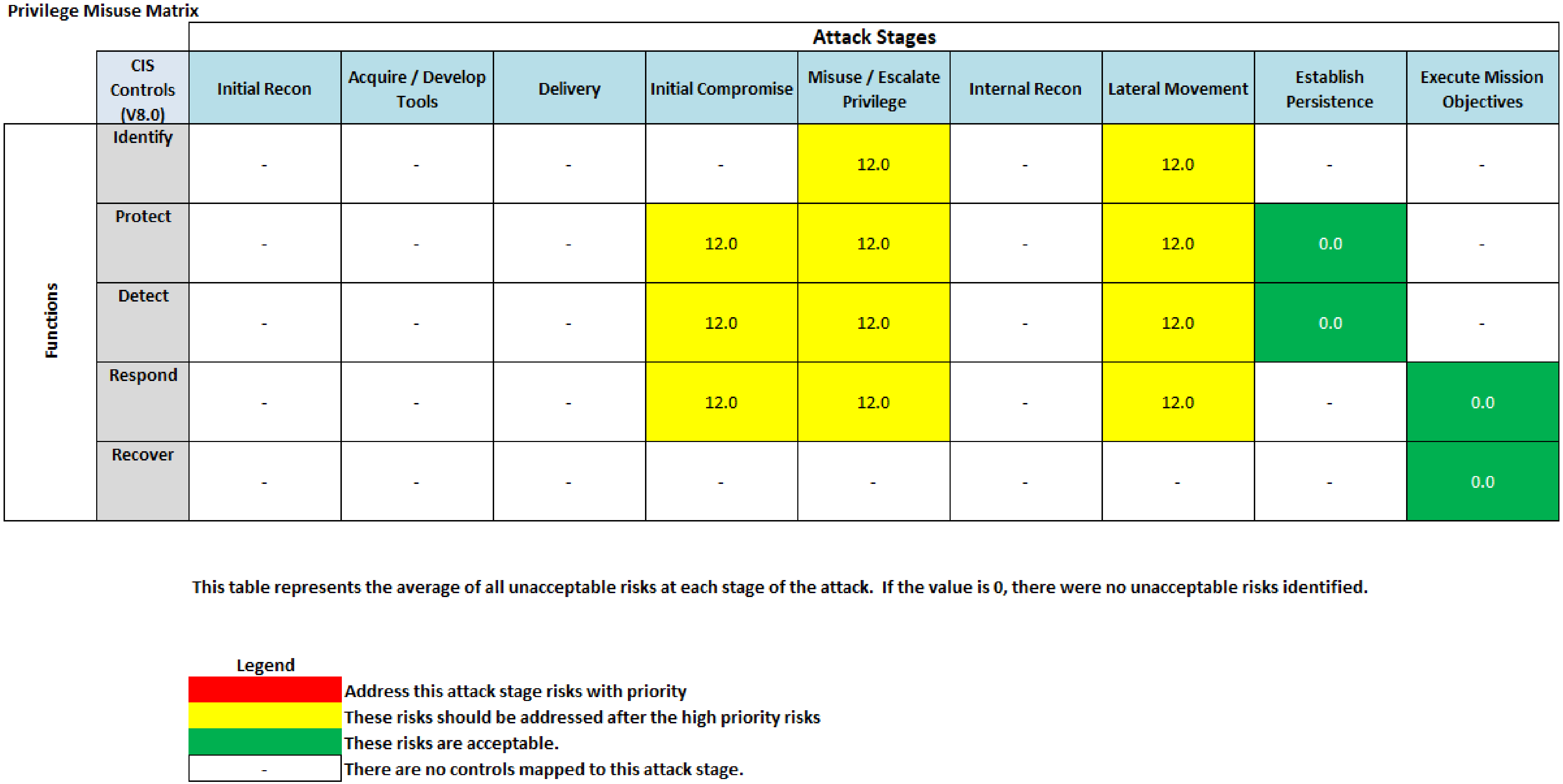
		Attack Stages								
	CIS Controls (V8.0)	Initial Recon	Acquire / Develop Tools	Delivery	Initial Compromise	Misuse / Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
Functions	Identify	🟩 0.0	🟩 0.0	-	🟨 12.0	🟨 12.0	-	🟨 12.0	-	-
	Protect	🟨 13.3	-	🟩 0.0	🟨 12.0	🟨 12.0	🟩 0.0	🟨 12.0	🟩 0.0	🟩 0.0
	Detect	-	-	🟩 0.0	🟨 12.0	🟨 12.0	🟩 0.0	🟨 12.0	🟩 0.0	🟩 0.0
	Respond	-	-	-	🟨 12.0	🟨 12.0	-	🟨 12.0	-	🟩 0.0
	Recover	-	-	-	-	-	-	-	-	🟩 0.0

This table represents the average of all UNACCEPTABLE risks at each stage of the attack. If the value is 0, there were no unacceptable risks identified.

Legend

🟥	Address this attack stage risks with priority
🟨	These risks should be addressed after the high priority risks
🟩	These risks are acceptable.
-	There are no controls mapped to this attack stage.

MITRE ATT&CK Mapping – Privilege Misuse Matrix



Privilege Misuse Matrix

		Attack Stages								
	CIS Controls (V8.0)	Initial Recon	Acquire / Develop Tools	Delivery	Initial Compromise	Misuse / Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
Functions	Identify	-	-	-	-	12.0	-	12.0	-	-
	Protect	-	-	-	12.0	12.0	-	12.0	0.0	-
	Detect	-	-	-	12.0	12.0	-	12.0	0.0	-
	Respond	-	-	-	12.0	12.0	-	12.0	-	0.0
	Recover	-	-	-	-	-	-	-	-	0.0

This table represents the average of all unacceptable risks at each stage of the attack. If the value is 0, there were no unacceptable risks identified.

Legend	
🟥	Address this attack stage risks with priority
🟨	These risks should be addressed after the high priority risks
🟩	These risks are acceptable.
-	There are no controls mapped to this attack stage.

Roadmap toward acceptable risk

Year	Initiatives	Risk Reduction
2024	1. Secure Application Development 2. Vulnerability Management 3. Third Party Security 4. System Management 5. Network Architecture 6. Application Management	32 Risk Points 28 Risk Points 6 Risk Points 6 Risk Points 6 Risk Points 6 Risk Points
2025	6 initiatives (to be selected in Q4.2024)	
2026	6 initiatives (to be selected in Q4.2025)	

What Controls Are We Improving in 2024?

Secure Application Development

Why this is important Improving secure application development is critical to reducing vulnerabilities, as current processes lack comprehensive SAST/DAST scanning and depend heavily on manual testing, increasing security risks.

Vulnerability Management

Why this is important Lack of dedicated resources and delayed remediation cycles hinder timely identification and resolution of critical security risks.

Third Party Security

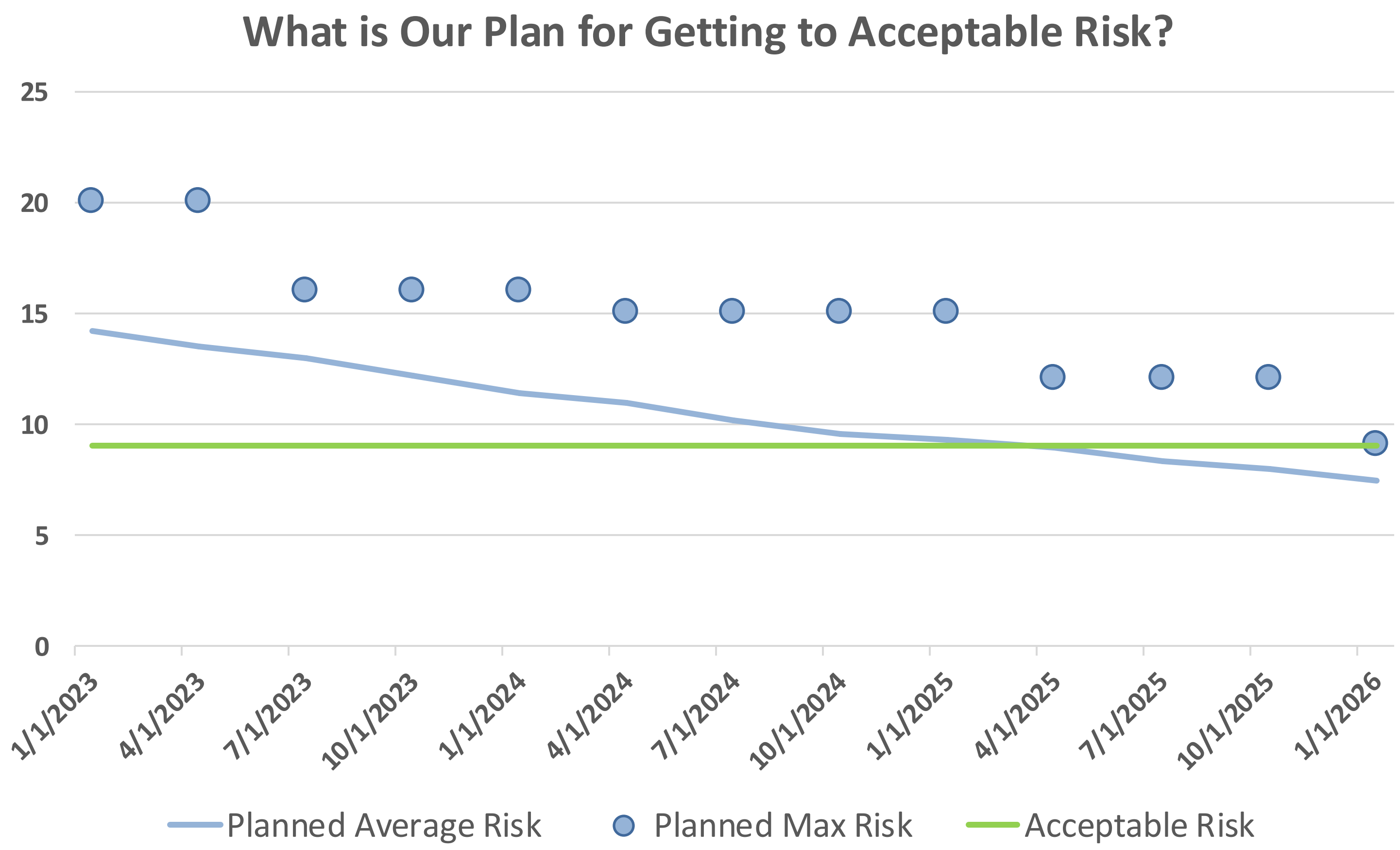
Why this is important Enhancing third-party security is vital, as continuous vendor monitoring is lacking, and reliance on vendor notifications increases the risk of unaddressed vulnerabilities in critical services.

What Controls Are We Improving in 2024?

System Management		
	Why this is important	Improving system management is crucial to integrate fragmented monitoring tools, enable baseline analysis, and ensure consistent configuration control for timely detection and resolution of issues.
Network Architecture		
	Why this is important	The company's network architecture is robust, with segmentation, SD-WAN, and firewall protections, but enhancing integrated monitoring and automated threat detection would further strengthen network security.
Application Management		
	Why this is important	Application management is well-structured with role-based access and Azure API security, but further integration of SSO and vulnerability scanning tools is essential for enhanced security.

How are We Measuring and Reporting Risk Reduction?

- Each year will have a risk reduction plan.
- For every control that is improved the associated risk AND the aggregated risk go down.
- The plan and the actual completion can be compared to determine whether more resources or new prioritization is needed.



Example

Questions