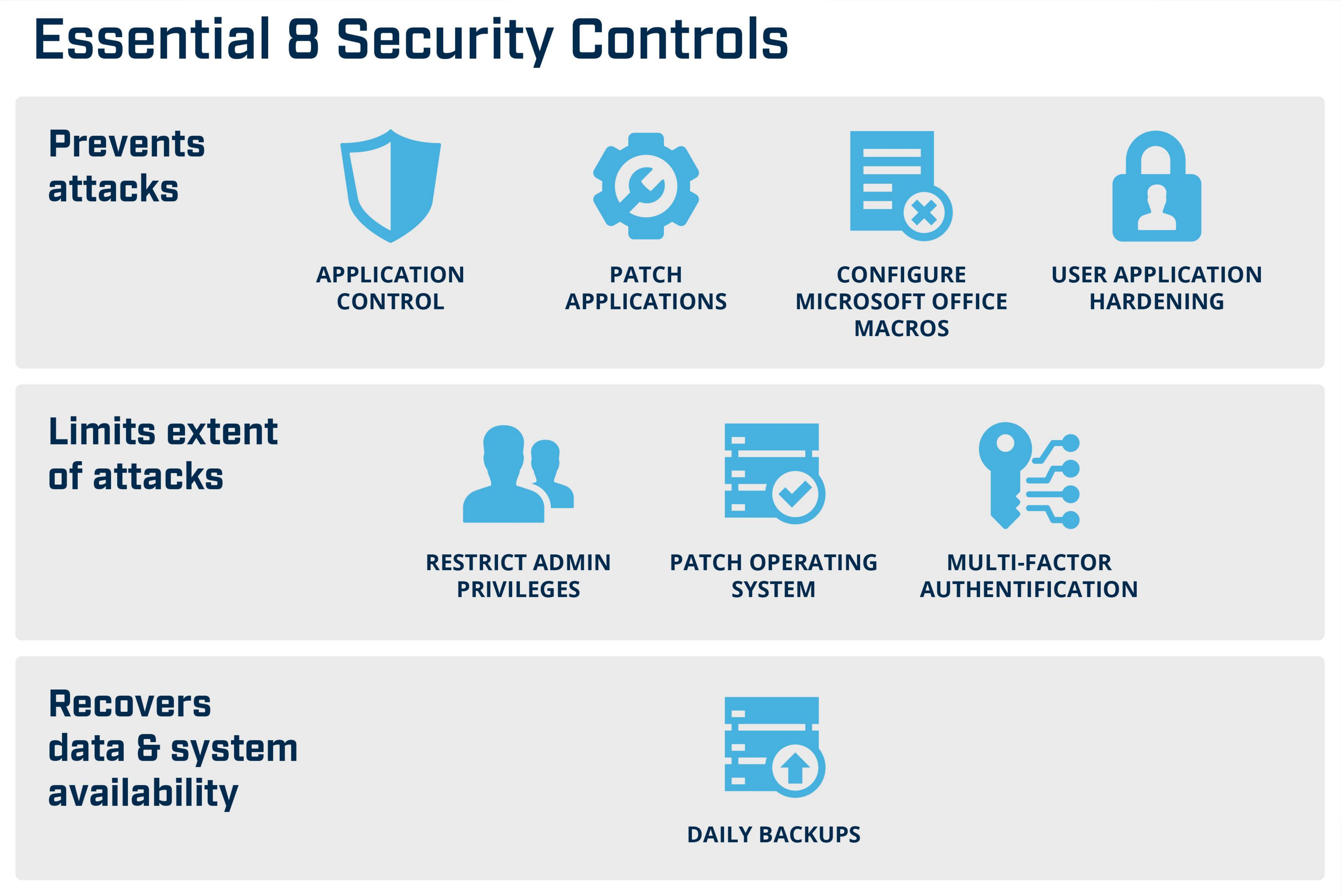
4walls
cyber advisory

Governance - Training and induction.

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

Making sense of it all



Essential 8 Security Controls

Prevents attacks

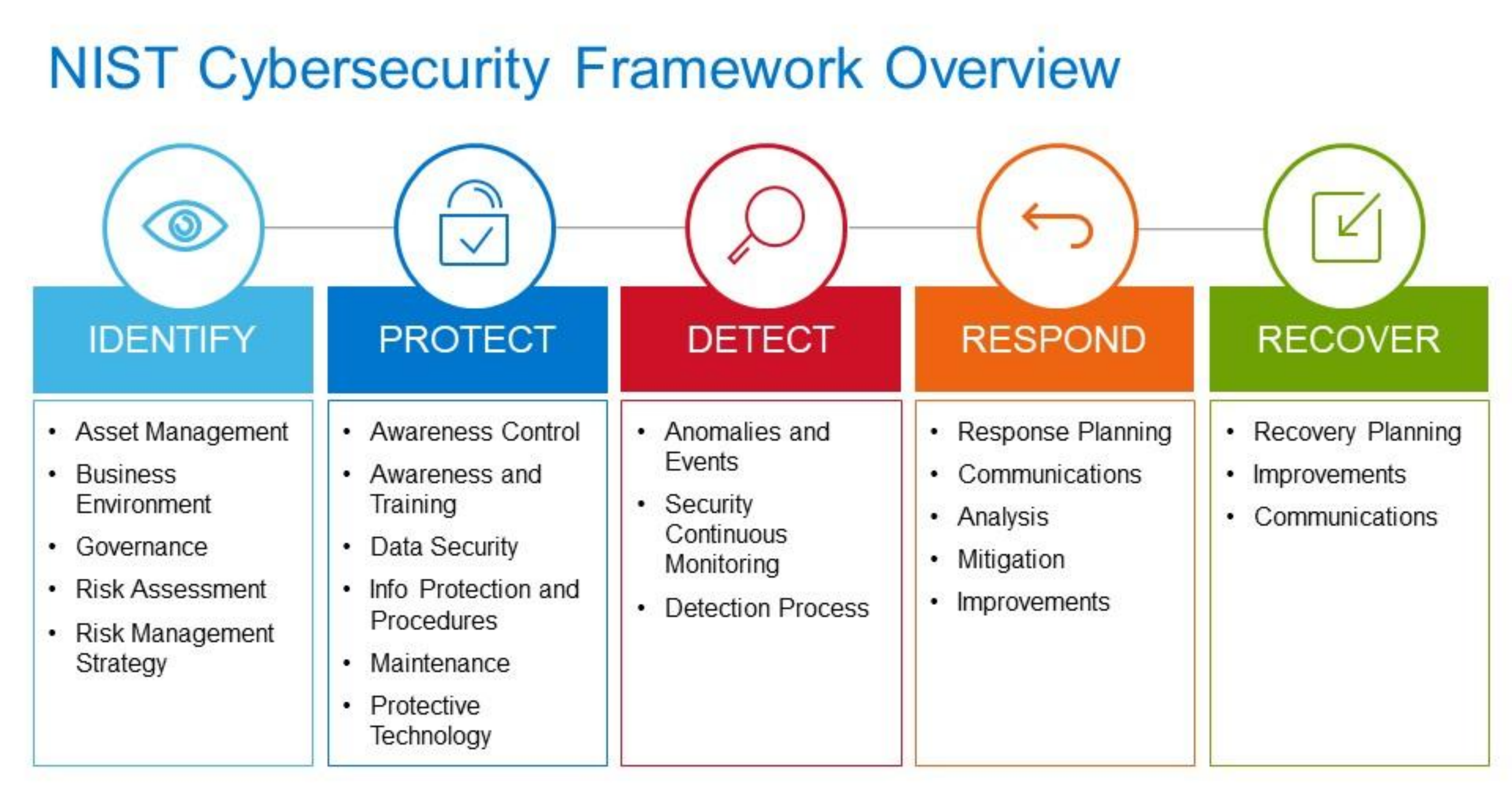
- APPLICATION CONTROL
- PATCH APPLICATIONS
- CONFIGURE MICROSOFT OFFICE MACROS
- USER APPLICATION HARDENING

Limits extent of attacks

- RESTRICT ADMIN PRIVILEGES
- PATCH OPERATING SYSTEM
- MULTI-FACTOR AUTHENTIFICATION

Recovers data & system availability

- DAILY BACKUPS



NIST Cybersecurity Framework Overview

IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Awareness Control
- Awareness and Training
- Data Security
- Info Protection and Procedures
- Maintenance
- Protective Technology

DETECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery Planning
- Improvements
- Communications

AICD Cyber Security Governance Principles

1. Set clear roles and responsibilities
2. Develop, implement and evolve a comprehensive cyber strategy
3. Embed cyber security in existing risk management practices
4. Promote a culture of cyber resilience
5. Plan for a significant cyber security event

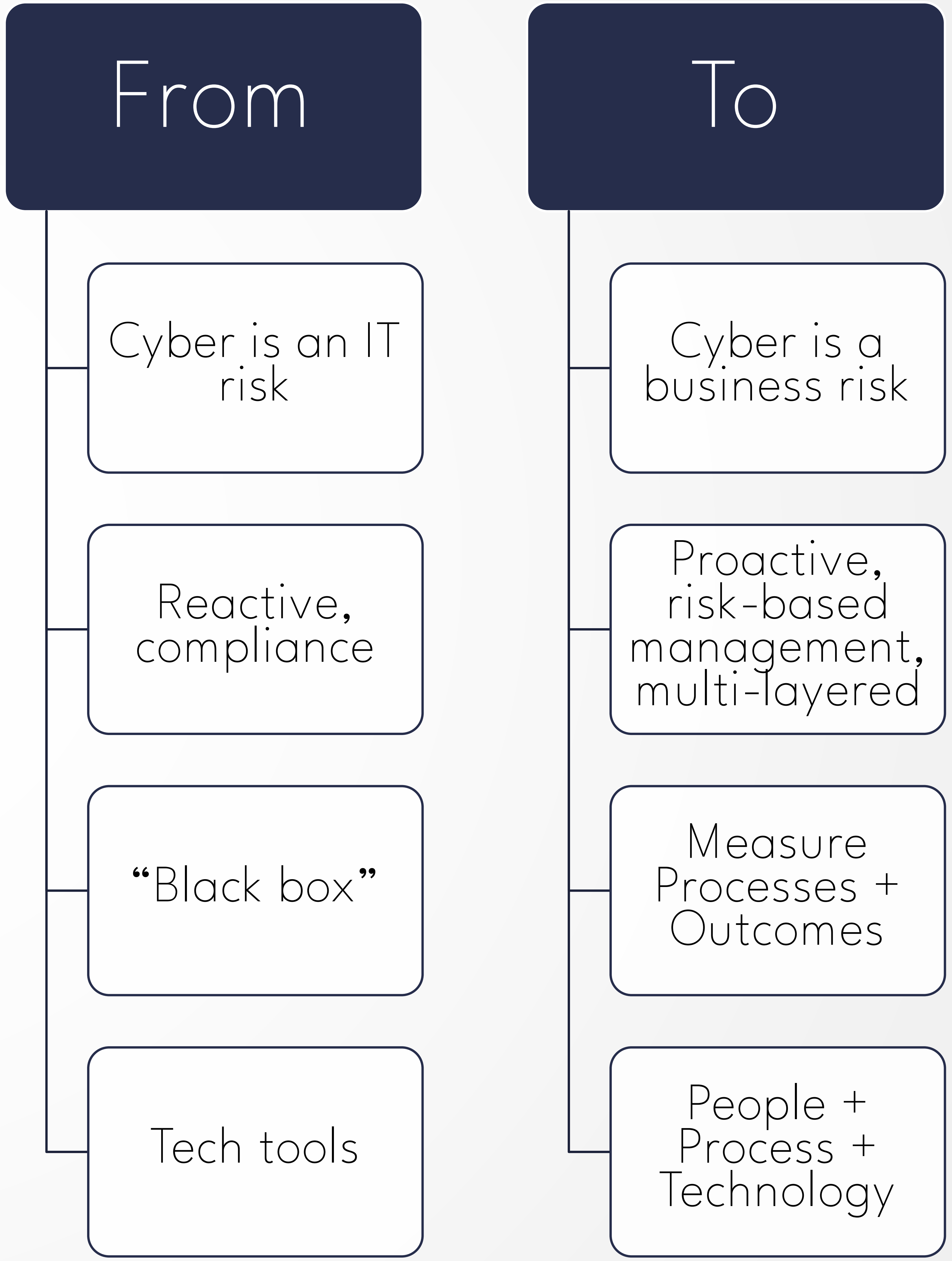
Building a Secure Culture

From the top:

- Leverage your existing risk oversight

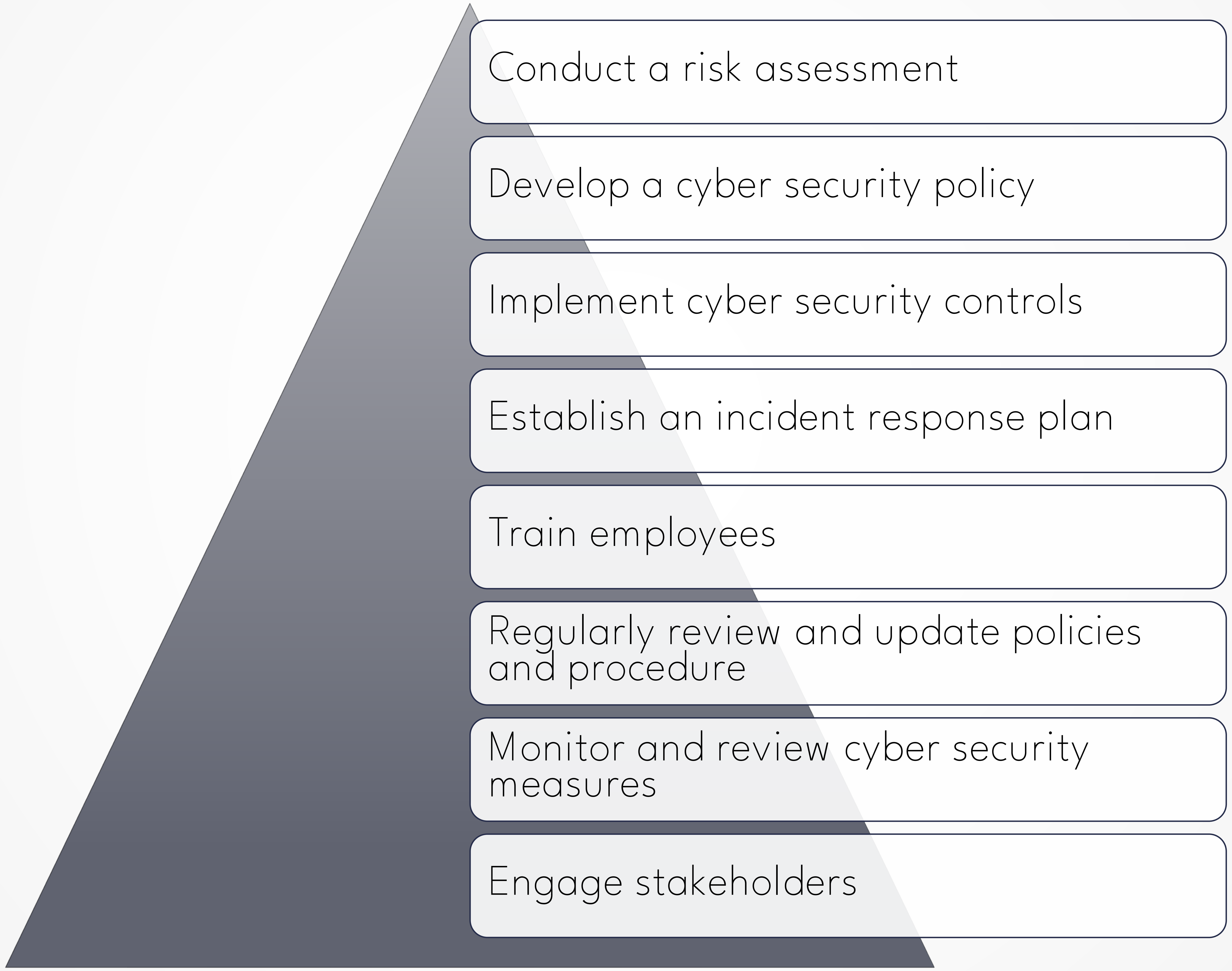
Mindset and Accountability:

- People first
  - 80% of threat comes from people
    AND
  - People are the strongest control



From	To
Cyber is an IT risk	Cyber is a business risk
Reactive, compliance	Proactive, risk-based management, multi-layered
“Black box”	Measure Processes + Outcomes
Tech tools	People + Process + Technology

Core Cyber Governance Principles
Practical (reasonable?) steps



- Conduct a risk assessment
- Develop a cyber security policy
- Implement cyber security controls
- Establish an incident response plan
- Train employees
- Regularly review and update policies and procedure
- Monitor and review cyber security measures
- Engage stakeholders

Core Cyber Governance Principles

Conduct a risk assessment	Identify and prioritise potential cyber risks to the organisation and determine appropriate measures to manage those risks
Develop a cyber security policy	That outlines the organisation's approach to cyber security governance, including roles and responsibilities, incident response procedures and compliance requirements
Implement cyber security controls	Based on the organisation's unique risk profile and the results of the risk assessment, such as firewalls, encryption and multi-factor authentication
Establish an incident response plan	That outlines procedures for responding to a cyber incident, including identifying the incident, containing the damage and reporting the incident to the appropriate authorities
Train employees	Educate and train employees on cyber security best practices
Regularly review and update policies and procedure	To ensure they remain effective and aligned with emerging threats and changes in the organisation's risk profile
Monitor and review cyber security measures	To ensure their effectiveness and identity areas for improvement
Engage stakeholders	Ensure that cyber security governance is a shared responsibility with all stakeholders playing a role in protecting the organisation's assets and data

Through a Director’s lens

Risk Management Framework

- Are cyber risks an integral part of the organisation’s risk management framework?
- How often is the cyber resilience program reviewed at board level?

Identifying cyber risk

- What risk is posed by cyber threats to the organisation’s business?
- Does the board need further expertise to understand the risk?

Monitoring cyber risk

- How can cyber risk be monitored and what escalation triggers should be adopted?

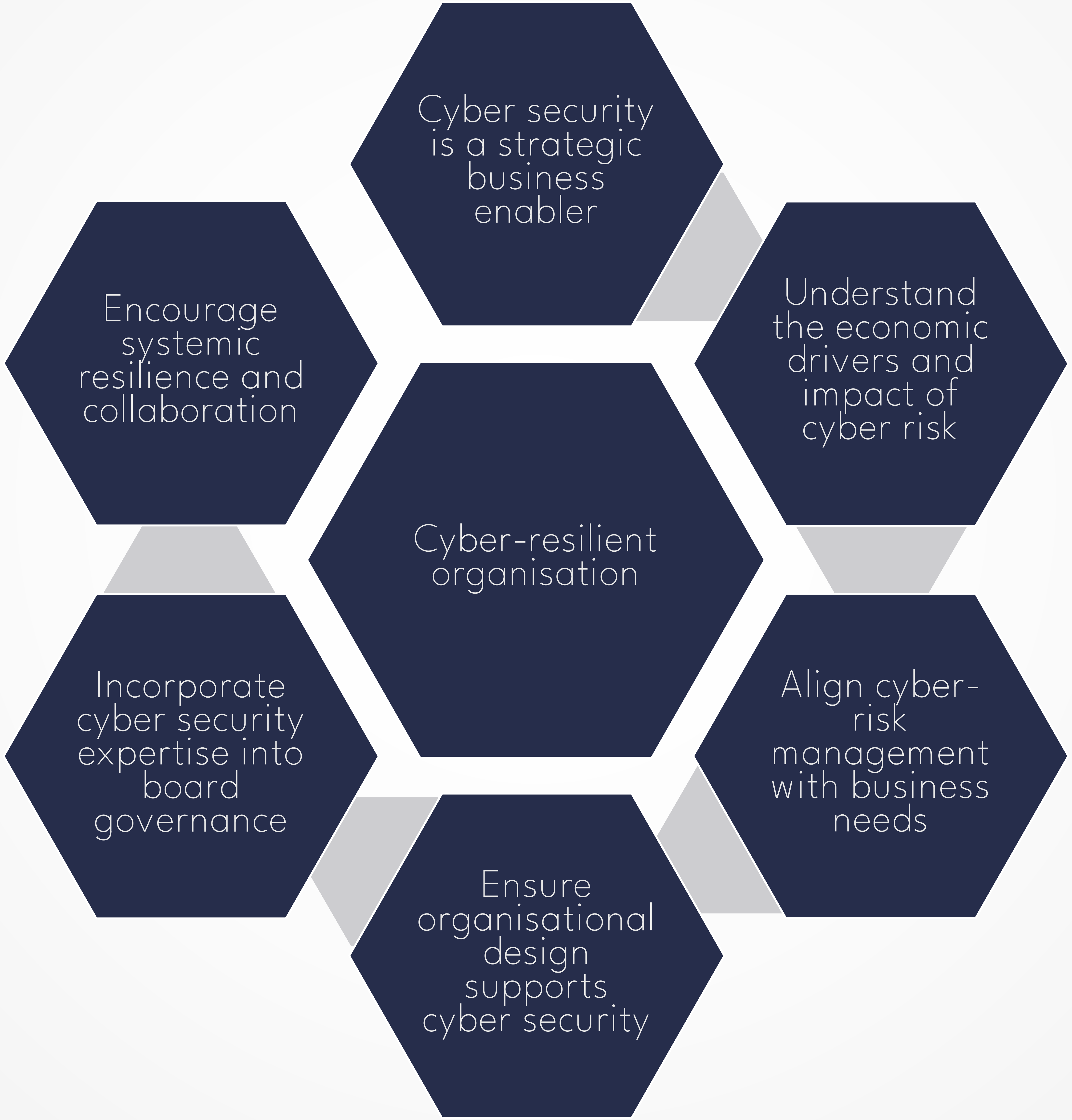
Controls

- What is the people strategy around cyber security?
- What is in place to protect critical information assets?

Response

- What needs to occur in the event of a breach?

End goal: Cyber-resilient organisation



Cyber security is a strategic business enabler

Understand the economic drivers and impact of cyber risk

Align cyber-risk management with business needs

Ensure organisational design supports cyber security

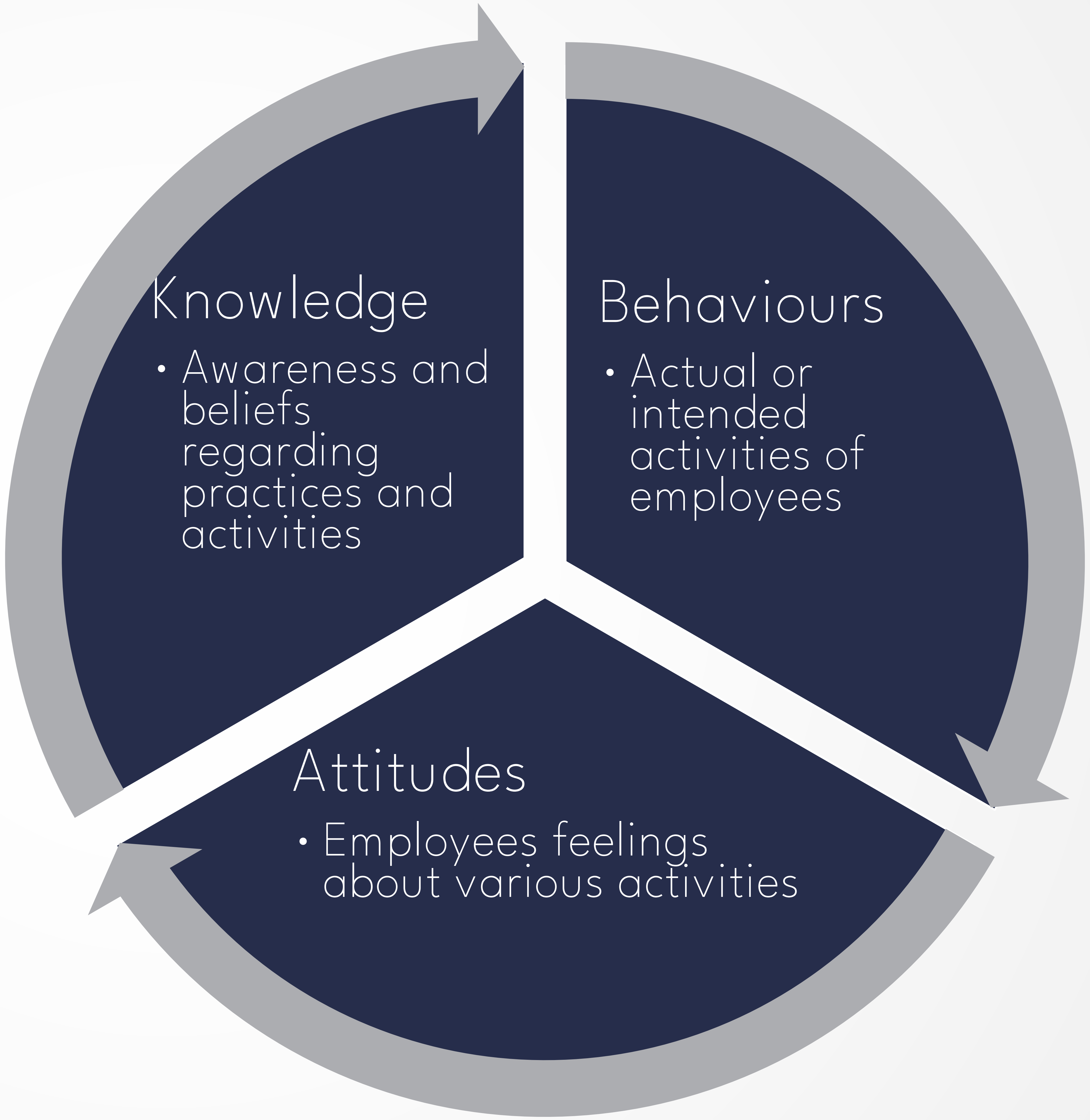
Incorporate cyber security expertise into board governance

Encourage systemic resilience and collaboration

Cyber-resilient organisation

Build a Secure Culture

1. Cyber Strategy
   - KPIs
   - Policies
   - Board reports
   - Technology
2. Training
   - Simulations
   - Education
3. Planning
   - Communication
   - Scenarios



Knowledge

- Awareness and beliefs regarding practices and activities

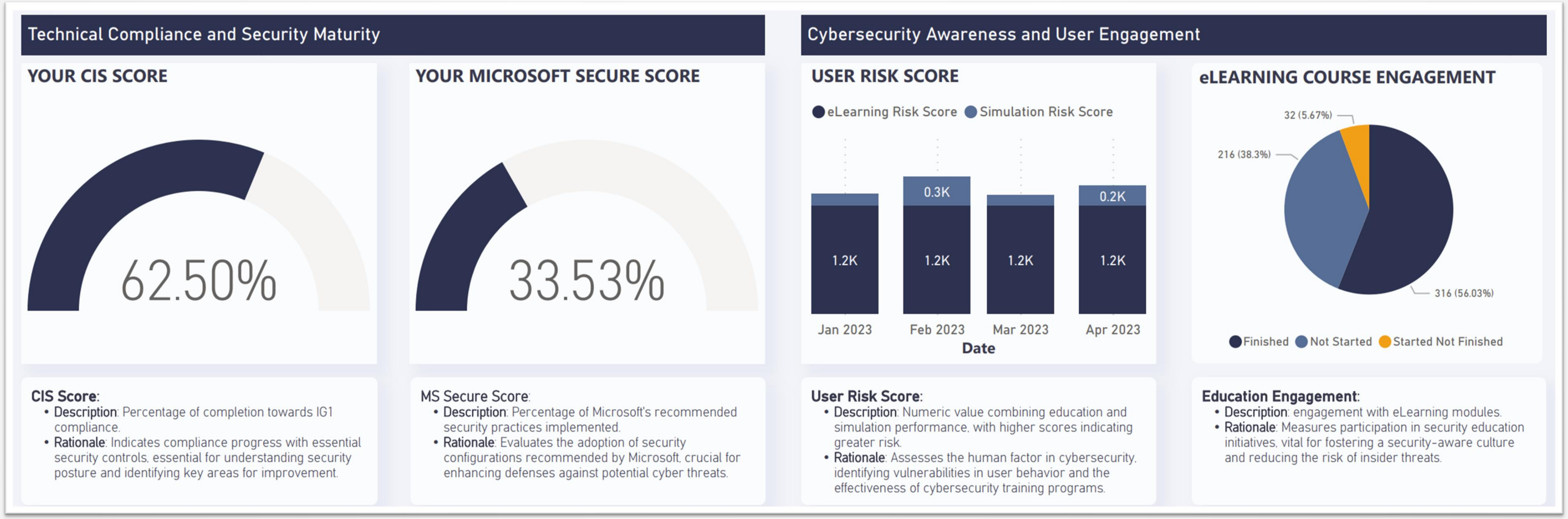
Behaviours

- Actual or intended activities of employees

Attitudes

- Employees feelings about various activities

Cyber Strategy:
KPIs, reports, dashboards



Technical Compliance and Security Maturity

CIS Score:
- **Description**: Percentage of completion towards IG1 compliance.
- **Rationale**: Indicates compliance progress with essential security controls, essential for understanding security posture and identifying key areas for improvement.

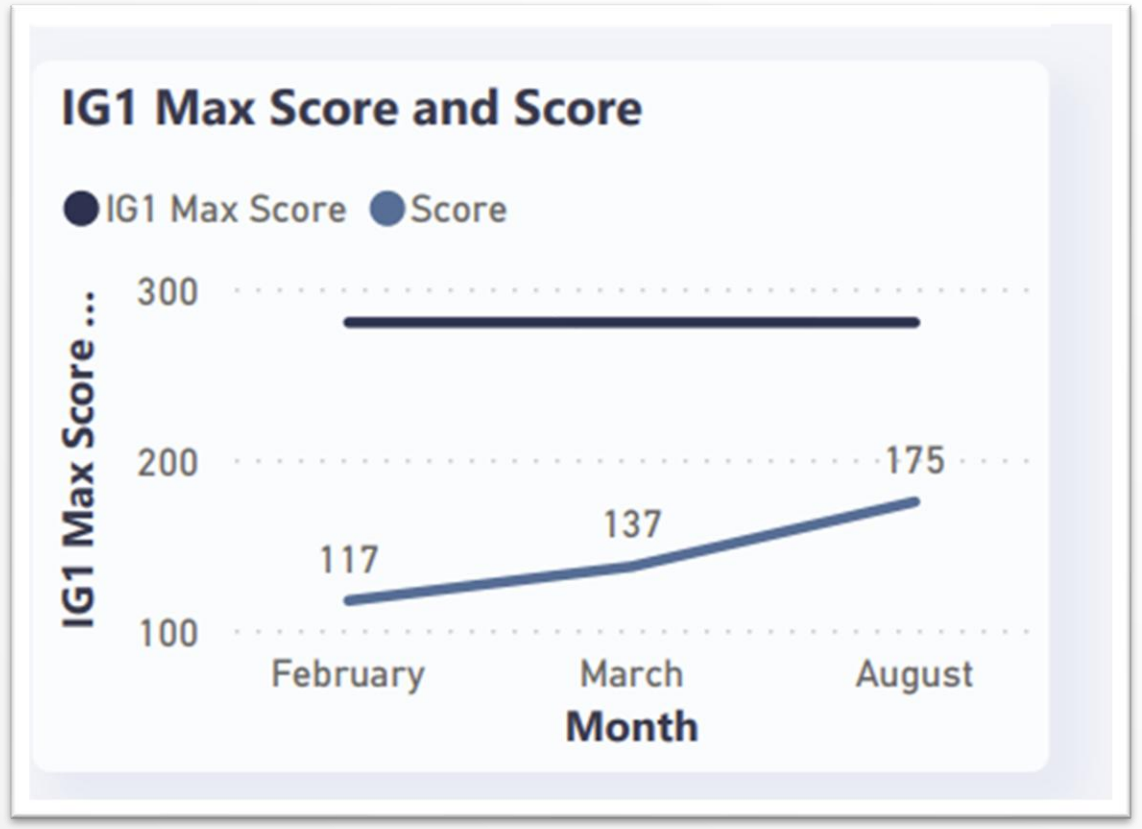
MS Secure Score:
- **Description**: Percentage of Microsoft's recommended security practices implemented.
- **Rationale**: Evaluates the adoption of security configurations recommended by Microsoft, crucial for enhancing defenses against potential cyber threats.

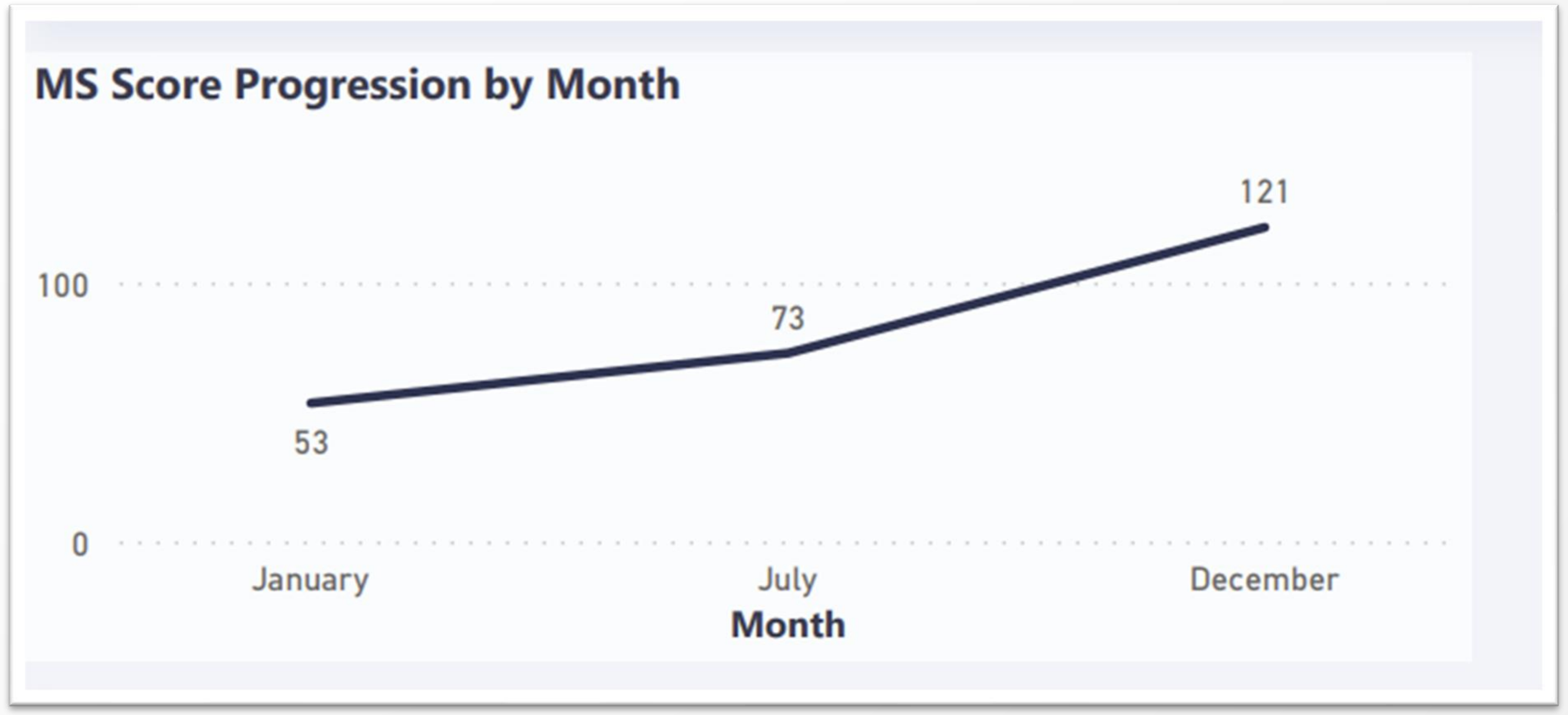
Cybersecurity Awareness and User Engagement

USER RISK SCORE
● eLearning Risk Score ● Simulation Risk Score
1.2K
0.3K
1.2K
1.2K
0.2K
1.2K
Jan 2023
Feb 2023
Mar 2023
Apr 2023
Date
eLEARNING COURSE ENGAGEMENT
32 (5.67%)
216 (38.3%)
316 (56.03%)
● Finished ● Not Started ● Started Not Finished

User Risk Score:
- **Description**: Numeric value combining education and simulation performance, with higher scores indicating greater risk.
- **Rationale**: Assesses the human factor in cybersecurity, identifying vulnerabilities in user behavior and the effectiveness of cybersecurity training programs.

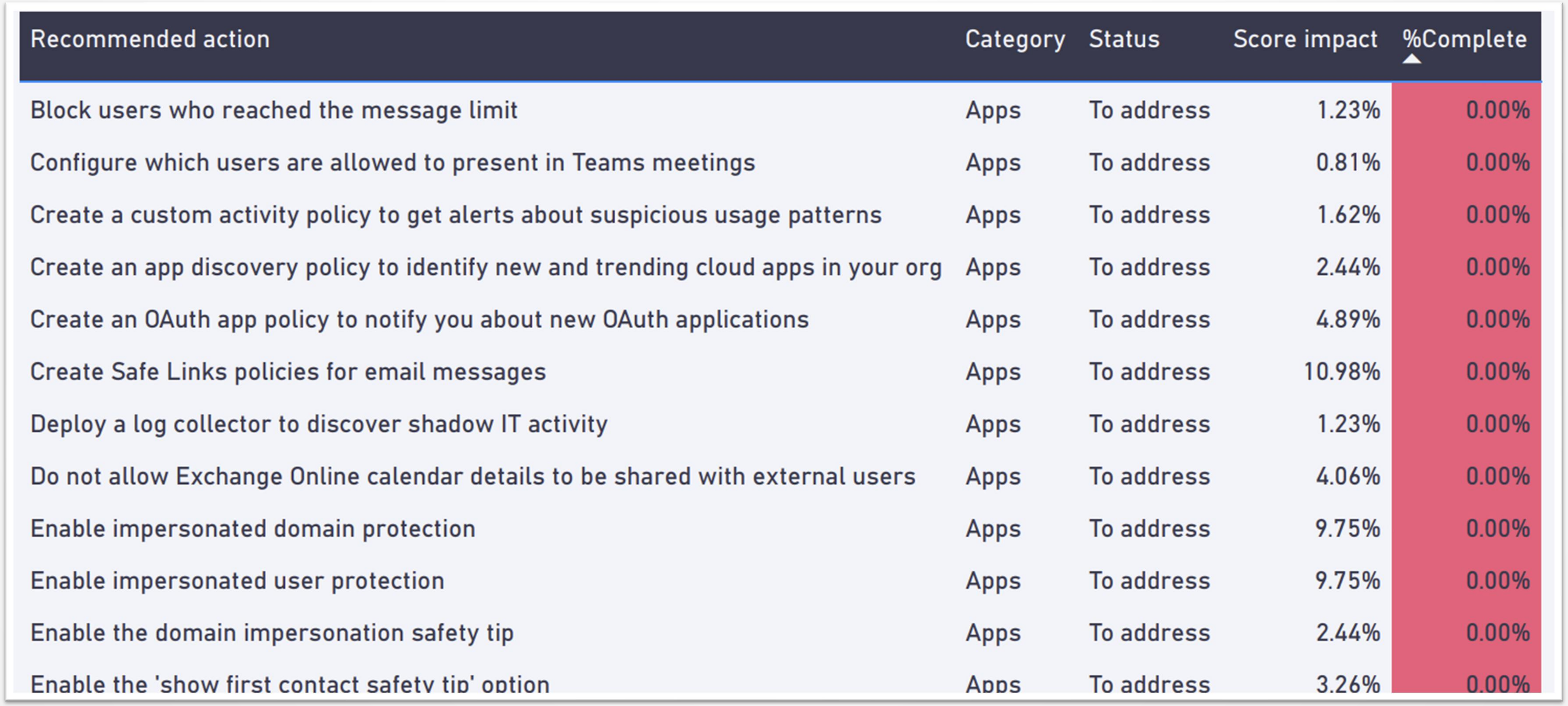
Education Engagement:
- **Description**: engagement with eLearning modules.
- **Rationale**: Measures participation in security education initiatives, vital for fostering a security-aware culture and reducing the risk of insider threats.





4walls
cyber advisory

Targeted action plans for focused improvement

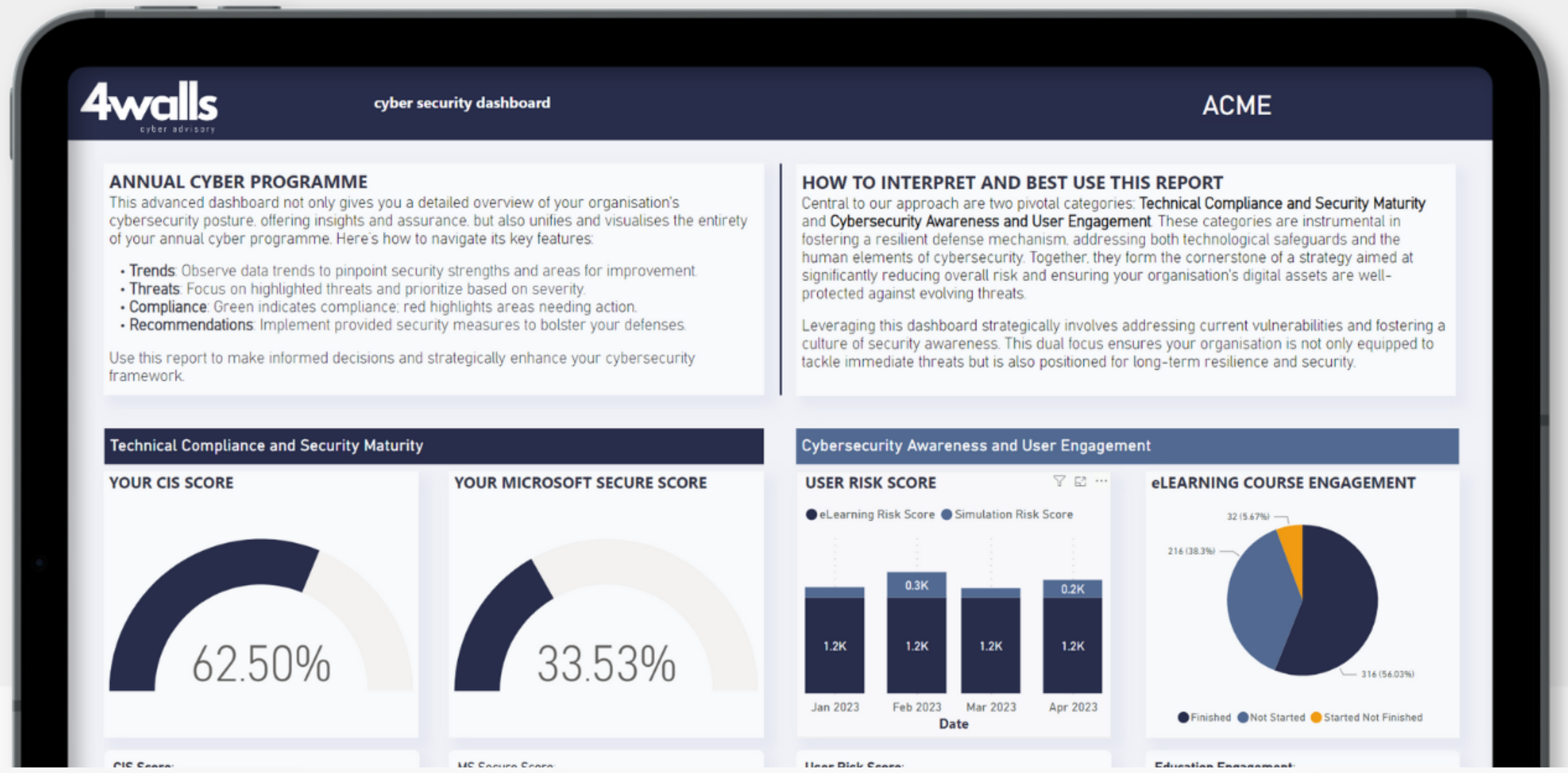


Recommended action	Category	Status	Score impact	%Complete
Block users who reached the message limit	Apps	To address	1.23%	0.00%
Configure which users are allowed to present in Teams meetings	Apps	To address	0.81%	0.00%
Create a custom activity policy to get alerts about suspicious usage patterns	Apps	To address	1.62%	0.00%
Create an app discovery policy to identify new and trending cloud apps in your org	Apps	To address	2.44%	0.00%
Create an OAuth app policy to notify you about new OAuth applications	Apps	To address	4.89%	0.00%
Create Safe Links policies for email messages	Apps	To address	10.98%	0.00%
Deploy a log collector to discover shadow IT activity	Apps	To address	1.23%	0.00%
Do not allow Exchange Online calendar details to be shared with external users	Apps	To address	4.06%	0.00%
Enable impersonated domain protection	Apps	To address	9.75%	0.00%
Enable impersonated user protection	Apps	To address	9.75%	0.00%
Enable the domain impersonation safety tip	Apps	To address	2.44%	0.00%
Enable the 'show first contact safety tip' option	Apps	To address	3.26%	0.00%

4walls cyber dashboard

cyber insights and assurance

behavioural insights and robust security assurance in one powerful dashboard... introducing the 4walls cyber dashboard



ANNUAL CYBER PROGRAMME

This advanced dashboard not only gives you a detailed overview of your organisation's cybersecurity posture, offering insights and assurance, but also unifies and visualises the entirety of your annual cyber programme. Here's how to navigate its key features:

- **Trends**: Observe data trends to pinpoint security strengths and areas for improvement.
- **Threats**: Focus on highlighted threats and prioritize based on severity.
- **Compliance**: Green indicates compliance; red highlights areas needing action.
- **Recommendations**: Implement provided security measures to bolster your defenses.

Use this report to make informed decisions and strategically enhance your cybersecurity framework.

HOW TO INTERPRET AND BEST USE THIS REPORT

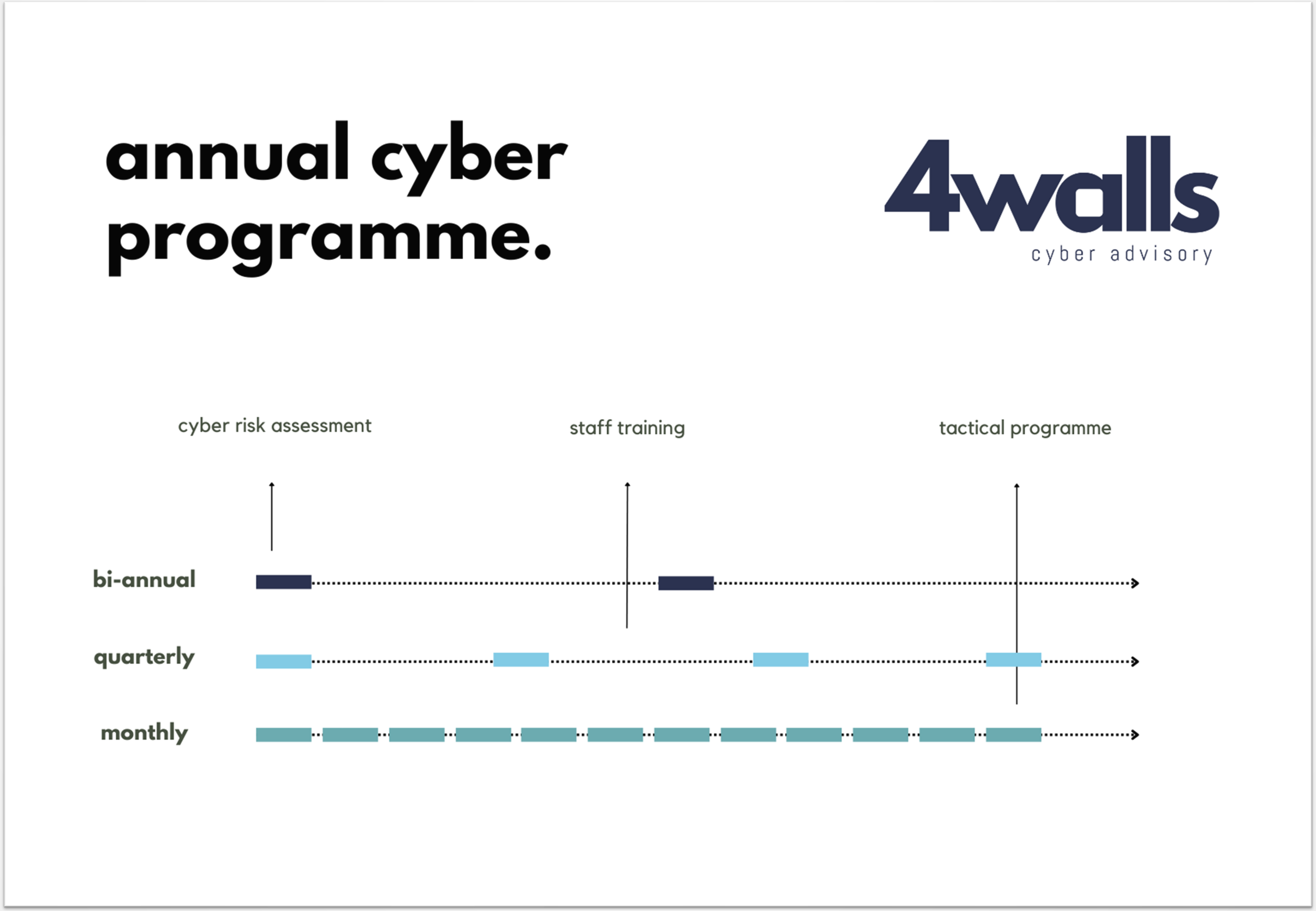
Central to our approach are two pivotal categories: **Technical Compliance and Security Maturity** and **Cybersecurity Awareness and User Engagement**. These categories are instrumental in fostering a resilient defense mechanism, addressing both technological safeguards and the human elements of cybersecurity. Together, they form the cornerstone of a strategy aimed at significantly reducing overall risk and ensuring your organisation's digital assets are well-protected against evolving threats.

Leveraging this dashboard strategically involves addressing current vulnerabilities and fostering a culture of security awareness. This dual focus ensures your organisation is not only equipped to tackle immediate threats but is also positioned for long-term resilience and security.

Technical Compliance and Security Maturity
YOUR CIS SCORE
62.50%
YOUR MICROSOFT SECURE SCORE
33.53%
Cybersecurity Awareness and User Engagement
USER RISK SCORE
● eLearning Risk Score ● Simulation Risk Score
0.3K
0.2K
1.2K
1.2K
1.2K
1.2K
Jan 2023
Feb 2023
Mar 2023
Apr 2023
Date
eLEARNING COURSE ENGAGEMENT
32 (5.67%)
216 (38.3%)
316 (56.03%)
● Finished ● Not Started ● Started Not Finished
CIS Score:
MS Secure Score:
User Risk Score:
Education Engagement:

4walls
cyber dashboard

powered by Human Intelligence



annual cyber programme.

4walls
cyber advisory

cyber risk assessment

staff training

tactical programme

bi-annual

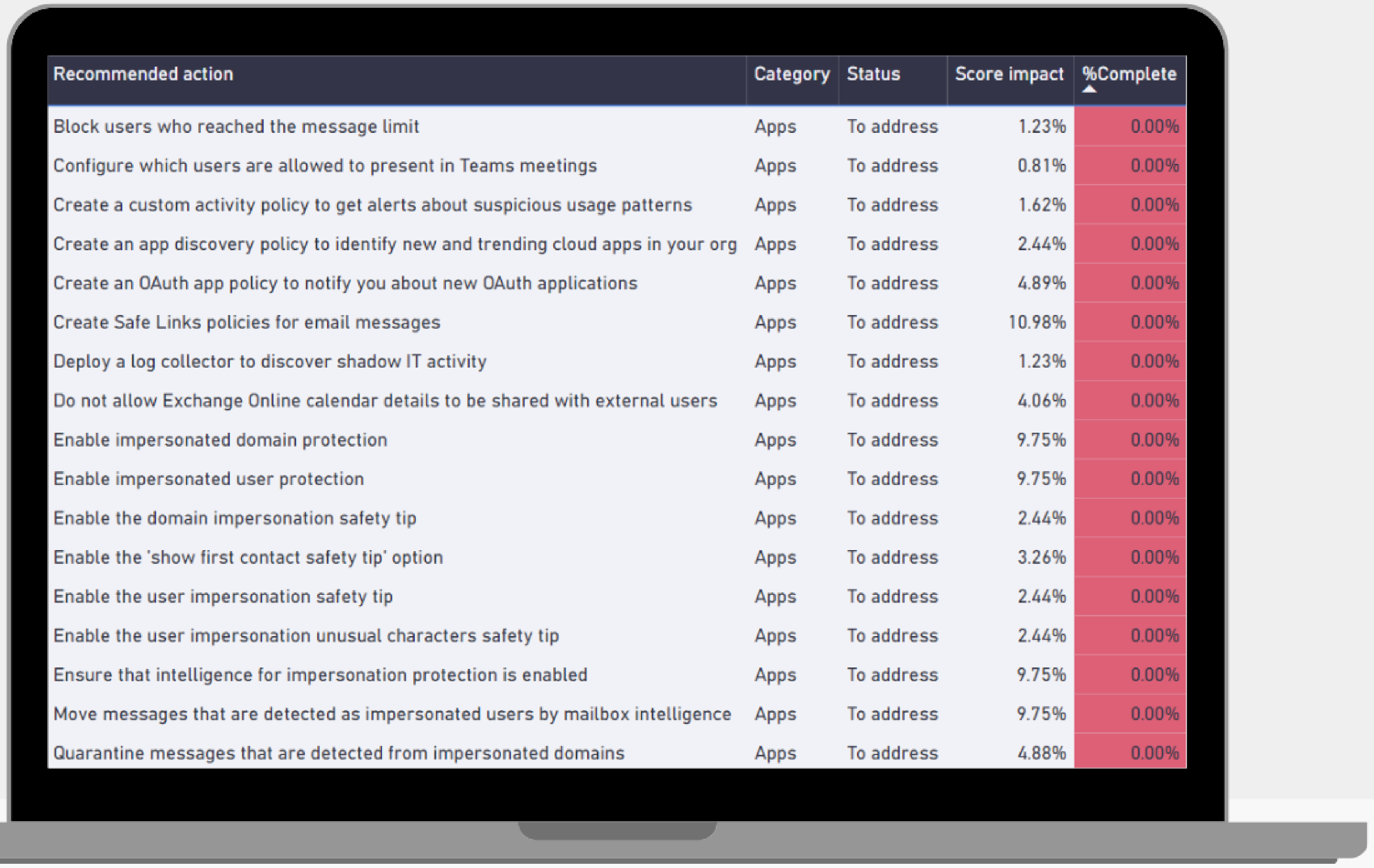
quarterly

monthly

4walls annual cyber programme

action

Drive decisive cybersecurity action with clear action plans, prioritised tasks based on risk impact, and progress tracking in real-time, empowering your organisation with proactive security management.



Recommended action	Category	Status	Score impact	%Complete
Block users who reached the message limit	Apps	To address	1.23%	0.00%
Configure which users are allowed to present in Teams meetings	Apps	To address	0.81%	0.00%
Create a custom activity policy to get alerts about suspicious usage patterns	Apps	To address	1.62%	0.00%
Create an app discovery policy to identify new and trending cloud apps in your org	Apps	To address	2.44%	0.00%
Create an OAuth app policy to notify you about new OAuth applications	Apps	To address	4.89%	0.00%
Create Safe Links policies for email messages	Apps	To address	10.98%	0.00%
Deploy a log collector to discover shadow IT activity	Apps	To address	1.23%	0.00%
Do not allow Exchange Online calendar details to be shared with external users	Apps	To address	4.06%	0.00%
Enable impersonated domain protection	Apps	To address	9.75%	0.00%
Enable impersonated user protection	Apps	To address	9.75%	0.00%
Enable the domain impersonation safety tip	Apps	To address	2.44%	0.00%
Enable the 'show first contact safety tip' option	Apps	To address	3.26%	0.00%
Enable the user impersonation safety tip	Apps	To address	2.44%	0.00%
Enable the user impersonation unusual characters safety tip	Apps	To address	2.44%	0.00%
Ensure that intelligence for impersonation protection is enabled	Apps	To address	9.75%	0.00%
Move messages that are detected as impersonated users by mailbox intelligence	Apps	To address	9.75%	0.00%
Quarantine messages that are detected from impersonated domains	Apps	To address	4.88%	0.00%