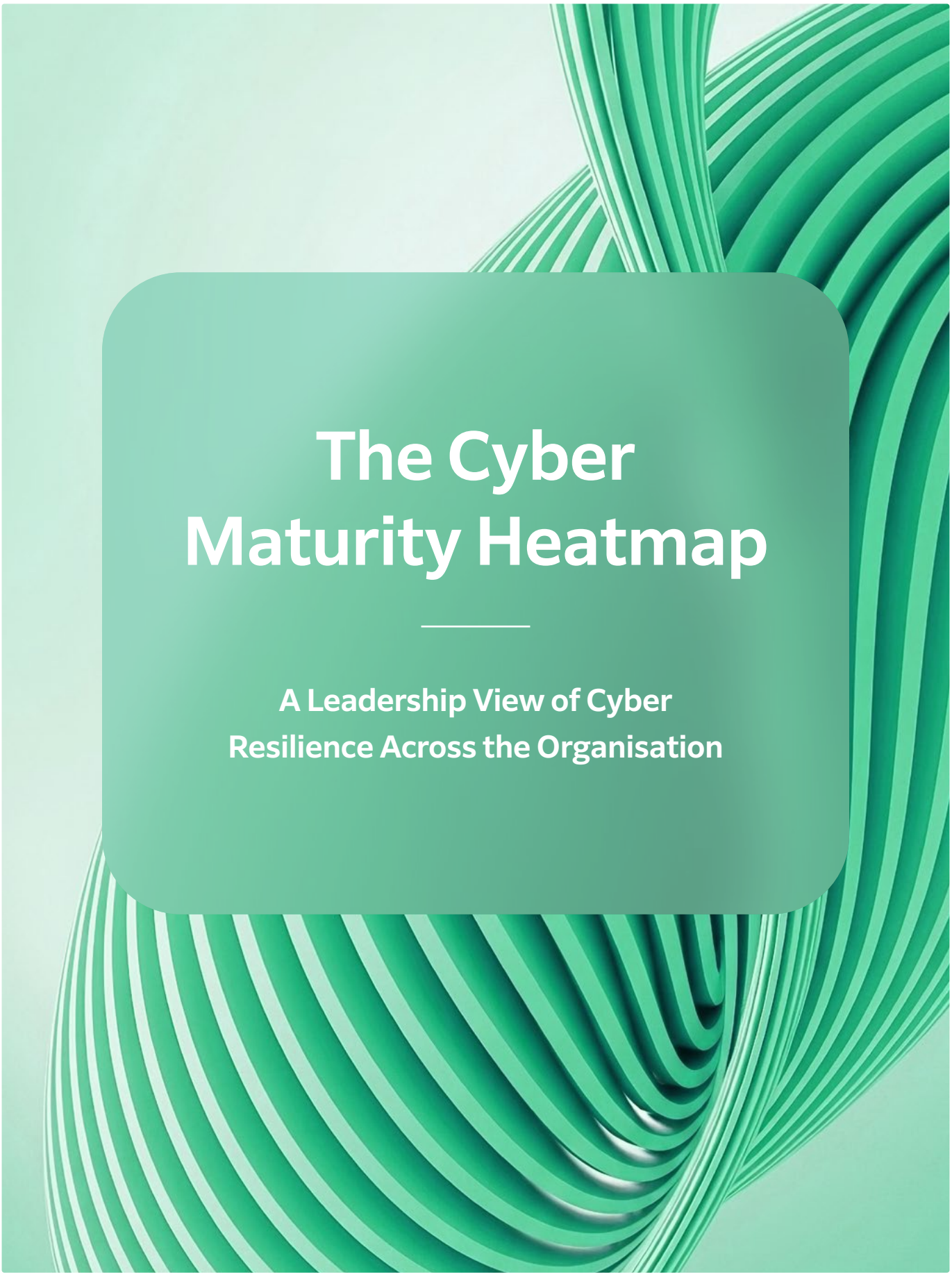
FUJIFILM
Value from Innovation

IT Services



# The Cyber Maturity Heatmap

## A Leadership View of Cyber Resilience Across the Organisation

# Benchmark Your Organisation's Cyber Resilience

Cybersecurity capability rarely develops evenly across an organisation.

Many organisations invest in security technologies, yet maturity often varies across governance, identity security, monitoring and response. As digital environments grow more complex, understanding where strengths and gaps exist becomes critical for managing cyber risk effectively.

The **Cyber Maturity Heatmap** provides a leadership-level benchmark for evaluating cybersecurity capability across thirteen core pillars of cyber resilience.

Use the heatmap below to assess where your organisation currently sits across five stages of cyber maturity.

## How to Use This Heatmap

The Cyber Maturity Heatmap is an indicative, self reported view of cyber maturity designed to support early discussion and orientation. It is not a validated assessment and should not be used as a definitive measure of cyber risk or control effectiveness.

Maturity should be interpreted by individual capability rather than total score. Strong performance in some areas can mask critical gaps in others, and low scoring domains may represent disproportionate cyber risk.

| Cyber Capability | Initial | Baseline | Defined & Consistent | Proactive & Managed | Resilient & Adaptive |
|---|---|---|---|---|---|
| End User Behaviour & Culture | Cyber awareness is largely informal, with limited training and little understanding of individual risk or responsibility. | Basic awareness training is delivered, but engagement varies and behaviours are not consistently reinforced. | Cyber behaviours are clearly defined, regularly trained, and embedded into day-to-day ways of working. | User behaviour is actively monitored and improved through targeted training, simulations and leadership reinforcement. | Cyber-aware behaviour is ingrained across the organisation, adapting continuously to emerging threats and business change. |
| Shadow IT & Application Landscape | Limited visibility of applications and tools in use, with widespread unmanaged or unauthorised systems. | Some discovery of applications occurs, but oversight and controls are inconsistent. | Application usage is documented, assessed and governed through defined processes. | Application risk is proactively managed, with continuous discovery and lifecycle controls. | The application landscape is continuously optimised and aligned to security, risk and business strategy. |
| Cyber Resilience | The organisation reacts to incidents with minimal preparation and limited recovery planning. | Basic recovery plans exist but are rarely tested or coordinated across the business. | Resilience strategies are defined, documented and regularly tested. | Cyber resilience is actively managed across people, process and technology. | The organisation adapts rapidly to disruption, learning from incidents and strengthening resilience over time. |
| Email & Threat Protection | Limited email filtering is in place, with high reliance on users to identify threats. | Standard filtering and basic user guidance reduce common threats. | Advanced protection tools and consistent user training are deployed organisation-wide. | Threats are proactively detected and responded to using behavioural analysis and automation. | Threat protection continuously evolves, integrating intelligence, automation and user behaviour insights. |
| Device & Patch Management | Devices are inconsistently managed, with irregular patching and limited visibility. | Patch management occurs but is manual and not always timely. | Devices are centrally managed with consistent patching and policy enforcement. | Device health and compliance are continuously monitored and optimised. | Device management dynamically adapts to risk, usage patterns and emerging vulnerabilities. |
| Data Security & Backups | Data protection and backups are informal, inconsistent or incomplete. | Backups are performed, but testing and recovery assurance are limited. | Data protection and backup processes are defined, tested and documented. | Data is proactively protected, monitored and recoverable across environments. | Data resilience is continuously assured, enabling rapid recovery and long-term trust. |
| Security Governance | Security responsibilities and policies are unclear or undocumented. | Some policies exist but are inconsistently applied or enforced. | Governance structures, roles and policies are clearly defined and aligned. | Governance is actively monitored, reviewed and improved. | Security governance evolves with business strategy, regulation and risk posture. |
| Identity & Access Management | Access is managed through basic credentials with limited oversight. | Stronger authentication exists but is inconsistently applied. | Access is centrally governed using role-based controls and MFA. | Identity risk is proactively monitored and managed across systems. | Identity controls adapt continuously to threat intelligence and business needs. |

| Cyber Capability | Initial | Baseline | Defined & Consistent | Proactive & Managed | Resilient & Adaptive |
|---|---|---|---|---|---|
| Risk & Governance | Cyber risk is addressed reactively with limited governance oversight. | Risk assessments occur but are ad hoc and not embedded into decision-making. | Cyber risk is formally assessed and integrated into governance processes. | Risk is actively managed across the enterprise, informing strategic decisions. | Cyber risk governance continuously adapts to changing threats and organisational priorities. |
| Monitoring & Incident Readiness | Limited monitoring exists, with minimal incident readiness. | Basic alerts are in place, but response processes are immature. | Monitoring and response processes are defined and regularly exercised. | Incidents are proactively detected and managed with automation and clear escalation. | Readiness continuously improves through learning, testing and intelligence-led monitoring. |
| Security Operations Management | Security operations are fragmented and reactive. | Some operational processes exist but lack consistency. | Security operations are defined, repeatable and centrally coordinated. | Operations are optimised through automation, metrics and continuous improvement. | Operations dynamically adapt to threat, scale and business transformation. |
| Resilience | Business disruption risk is not well understood or planned for. | Some resilience planning exists but is limited in scope. | Resilience is embedded into key systems and processes. | Resilience is actively managed across the organisation. | The organisation continuously adapts to disruption with confidence and agility. |
| Architecture & Strategy | Security architecture is patchwork and driven by short-term needs. | Some architectural planning exists but lacks cohesion. | A defined security architecture aligns to business and risk strategy. | Architecture is proactively optimised to support growth and resilience. | Security strategy and architecture continuously evolve alongside the business. |

# Calculate Your Cyber Maturity Score

Use the scoring system below to calculate your organisation's cyber maturity.

## Step 1 - Score Each Cyber Capability

Select the maturity level that best represents your organisation for each cyber capability and record the corresponding score.

| Maturity Level | Score |
|---|---|
| Initial | 1 point |
| Baseline | 2 points |
| Defined & Consistent | 3 points |
| Proactive & Managed | 4 points |
| Resilient & Adaptive | 5 points |

Capability descriptions are illustrative and should be interpreted in terms of outcomes achieved and risk reduced, rather than the presence of specific tools or technologies.

## Step 2 – Calculate Your Total Score

Add the scores from all thirteen cyber capability areas to calculate your total score.

**Your total score = Sum of all cyber capability scores**
**Maximum possible score: 65**

Low maturity scores do not necessarily mean controls are absent. In many cases, they reflect limited validation, inconsistent implementation or lack of assurance rather than a complete lack of capability.

## Step 3 – Understand Your Cyber Maturity

Use your total score to determine your organisation's cyber maturity level:

| Total Score | Overall Maturity Level | What It Indicates |
|---|---|---|
| 13-20 | Initial | Cyber capabilities are largely reactive and inconsistent, with limited formal governance or resilience. |
| 21-33 | Baseline | Foundational controls are in place, but practices are uneven and not yet embedded organisation-wide. |
| 34-46 | Defined & Consistent | Cyber practices are formally defined, documented and applied consistently across most areas. |
| 47-59 | Proactive & Managed | Cyber risk is actively managed, monitored and improved in alignment with business priorities. |
| 60-65 | Resilient & Adaptive | Cyber maturity is embedded into strategy and operations, enabling continuous adaptation to change and threat. |

Your overall cyber maturity level reflects how consistently higher-level practices are applied across all thirteen core cyber capability areas.

Many organisations find their cyber maturity varies across capability areas. As a result, even a strong overall score can mask critical gaps, and low scoring domains may represent disproportionate cyber risk.

## Identify Your Priority Improvements

Capabilities that fall within the initial or baseline stages represent the greatest areas of exposure and should be prioritised for improvement.

Focus first on areas where your organisation scored lowest, as these are most likely to impact your overall resilience.

Common key focus areas include:

- Identity governance and privileged access management
- Threat monitoring and detection capabilities
- Incident response readiness
- Backup and recovery resilience

Strengthening these key capabilities can significantly improve your organisation's ability to prevent, detect and respond to cyber threats.

## Benchmark Your Cyber Maturity

The Cyber Maturity Heatmap is intended as pre assessment material, designed to inform and focus a subsequent guided Cyber Maturity Assessment. The Cyber Maturity Heatmap provides a high-level snapshot of your organisation's current security posture across key capability areas.

However, many organisations find that a self-assessment only tells part of the story.

A Cyber Maturity Assessment provides a deeper, structured evaluation of your cyber environment, helping to validate your results and uncover gaps and vulnerabilities that may not be immediately visible.

This assessment looks across key areas including governance, identity, endpoint security, monitoring and response, and data protection.

**If you're unsure whether your results reflect your true level of cyber risk, a guided Cyber Maturity Assessment can provide clarity, direction and confidence in your next steps.**

### Learn More About the Cyber Maturity Assessment

**fujifilm.com/fbau**

FUJIFILM



**FUJIFILM Business Innovation Australia Pty Ltd**
Level 2, 54 Waterloo Road, Macquarie Park, NSW 2113 Australia
Contact us at fujifilm.com/fbau or 13 14 12