CYBER SECURITY - GRC

Cyber security frameworks:

Frameworks

Cyber risks are not just IT issues — they are major business risks. Organisations should choose a cybersecurity framework that aligns with their business strategy and priorities. Since most organisations outline their strategy in their annual reports, these should be reviewed before selecting a framework. If the framework does not align with the business strategy, it can be difficult to gain support and may work against the organisation's goals.

Most organisations have a business plan and strategy, and large organisations usually publish this in their annual report. A cybersecurity plan should align with the business strategy so both work together. When they are aligned, cybersecurity helps protect the organisation and supports it in achieving its business goals.

Adopting the framework: **The Essential Eight: The** Essential Eight is a cybersecurity risk-mitigation model created by the Australian Cyber Security Centre (ACSC). It helps organisations protect their systems from common cyber threats by focusing on the most important security actions.

The Essential Eight includes **eight key security controls** that:

- **Prevent cyber attacks**
- **Limit the damage if an attack occurs**
- **Help recover data and systems after an attack**

How the Essential Eight works:

- **Prevents attacks: Application** control, patching applications, configuring Microsoft Office macros, and hardening user applications help stop attacks before they happen.

- **Limits the impact of attacks: restricting** administrative privileges, patching operating systems, and using multi-factor authentication reduce how much damage an attacker can cause.
- **Recovers data and systems: daily** backups allow organisations to restore data and systems quickly after an incident.

Prevents attacks:

- Application control
- Patch applications
- Configure Microsoft Office macros
- User application hardening

Limits the impact of attacks:

- Restrict administrator privileges
- Patch operating systems
- Use multi-factor authentication

Recovers data and systems:

- Perform daily backups
-

Benchmarking against industry peers and maturity assessment.

- Once an organisation has completed a maturity assessment and benchmarking, the findings should be presented to internal stakeholders—such as the executive team—to communicate insights, align on priorities, and secure support for the proposed actions.

- Keep the message clear and concise, as stakeholders are often time-poor and may not have detailed technical knowledge.

Secure Room L3 Overview

Secure Room L3 Overview

The *Secure Room L3 Overview* is a simple status table used to show the board how cybersecurity controls are progressing.

- The **key** explains what each status means (Complete, In Progress, Blocked/Issues, Unknown).
- The rows list important security controls, such as **patching applications** and **Microsoft Office macro settings**.
- The columns (Endpoints, Servers, Application Control) show **where each control applies**.

This format lets leaders **quickly see what is finished, what is underway, and where there are problems**, without needing technical knowledge.

The need for change management:

The implementation of a cybersecurity framework can involve a big shift in work practices and also in the organisational culture. Therefore, the process needs effective change management so that employees understand the change and can effectively transition to new ways of working.

Change management is a systematic approach to dealing with the transition or transformation of organisational goals, processes and technology. The objective of change management is to implement methods to mitigate any risk to operations and manage the impact of the change within the organisation. Implementing a cyber plan and a cyber strategy requires a significant change management effort, as it is driving changes in the organisation. Generally, when an organisation goes through a large transformation, a robust change impact assessment is completed to understand the impact on all staff and customers.

Five key elements to change management are:

Clear communication

Leadership support

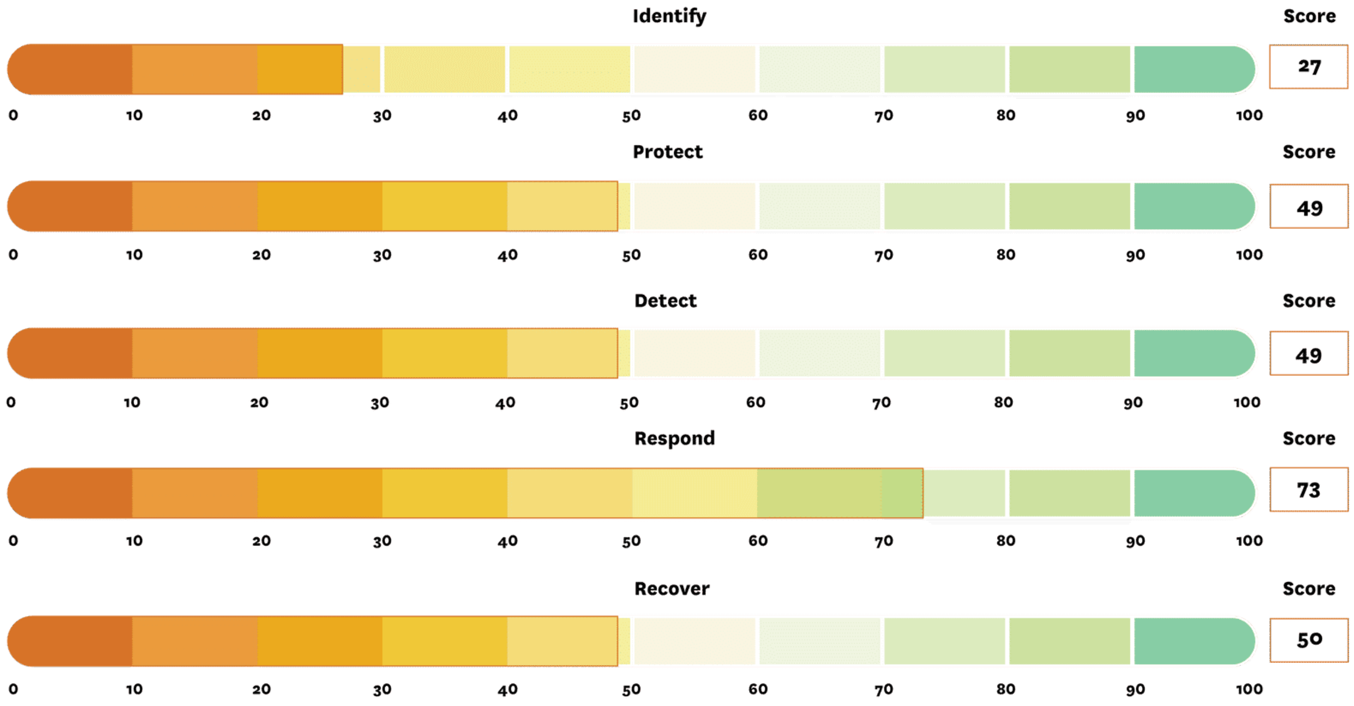
Training and awareness

Managing resistance to change

Ongoing monitoring and feedback

After a cybersecurity framework is implemented, leaders should receive regular progress updates so they can see how things are going and provide support if needed. These reports show how mature the organisation's cybersecurity is and what progress has been made.

For senior stakeholders, progress reports clearly show the current state and the target state. This helps them decide whether the work is on track or if changes—such as speeding up the timeline—are needed.



The diagram is an example of a **progress report** that shows how mature an organisation's cybersecurity is using the **NIST Cybersecurity Framework**.

Why the "Govern" function is missing

The chart shows only **five functions** (Identify, Protect, Detect, Respond, Recover). This is because it is based on **NIST CSF v1.1**.

2025 Context Note (important):
In **NIST CSF v2.0**, a new **Govern** function was added to highlight governance, risk management, and accountability. The diagram still uses the older version, but it is

included only to show **how progress and maturity can be reported visually**, not to reflect the latest framework structure.

How to read the bar chart

- Each bar shows how strong the organisation is in a cybersecurity area.
- Scores go from **0 to 100**:
    - **0** = controls are very basic or do not exist
    - **100** = controls are fully implemented and mature

What the scores mean

- Identify: **27/100**
- Protect: **49/100**
- Detect: **49/100**
- Respond: **73/100**
- Recover: **50/100**

For example, the **Identify** score is **27**.
If the organisation's target is **80**, it needs a **53-point improvement** to reach that goal.

Why targets differ

Target scores are set based on the organisation's **risk appetite** and **business goals**.
Different organisations accept different levels of risk, but similar organisations often aim for similar targets.

In short:
This chart helps leaders quickly see **where cybersecurity is strong, where it is weak, and how much improvement is needed**.

Board Reports:

A recent study by Lloyd's of London shows that **cyber risk is now one of the top three risks** facing organisations worldwide. Because of this, information security is now a **key part of business risk management** and a high priority for organisations.

The cybersecurity team should clearly explain the organisation's **current risk level**, the **security strategy**, and **what investment is needed** to reach the desired level of protection. Board reports are important because they help **tell this story** to executives and board members, who make the final decisions.

Good board reports use **simple, non-technical language**. Instead of focusing on technical details, they explain **what the risk is, why it matters to the business, and what actions are needed**.

Senior leaders mainly care about **business value and return on investment**. So, security investments should be explained in terms of benefits to the organisation—for example, better identity management improves security **and** increases customer trust.

Cybersecurity strategies and frameworks

Cybersecurity strategies and frameworks help organisations **protect their systems and data from cyber attacks**. For them to work well, they must **match the organisation's business goals**. This makes it easier to implement and get support from leadership.

Benchmarking—comparing with other organisations—is important. It helps a business **learn best practices** and make sure its security measures are up to date and meet industry standards.

Change management is also key. This means **keeping stakeholders informed** through progress updates and board reports so they stay committed, provide resources, and understand successes and challenges.

In short, a strong cybersecurity strategy should:

- Align with business goals
- Learn from industry peers
- Include good change management

Doing this helps businesses **protect their systems and data, maintain their reputation, and keep customer and partner trust**.