CYBER SECURITY - GRC

Cyber security frameworks:
GOVERNANCE:

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

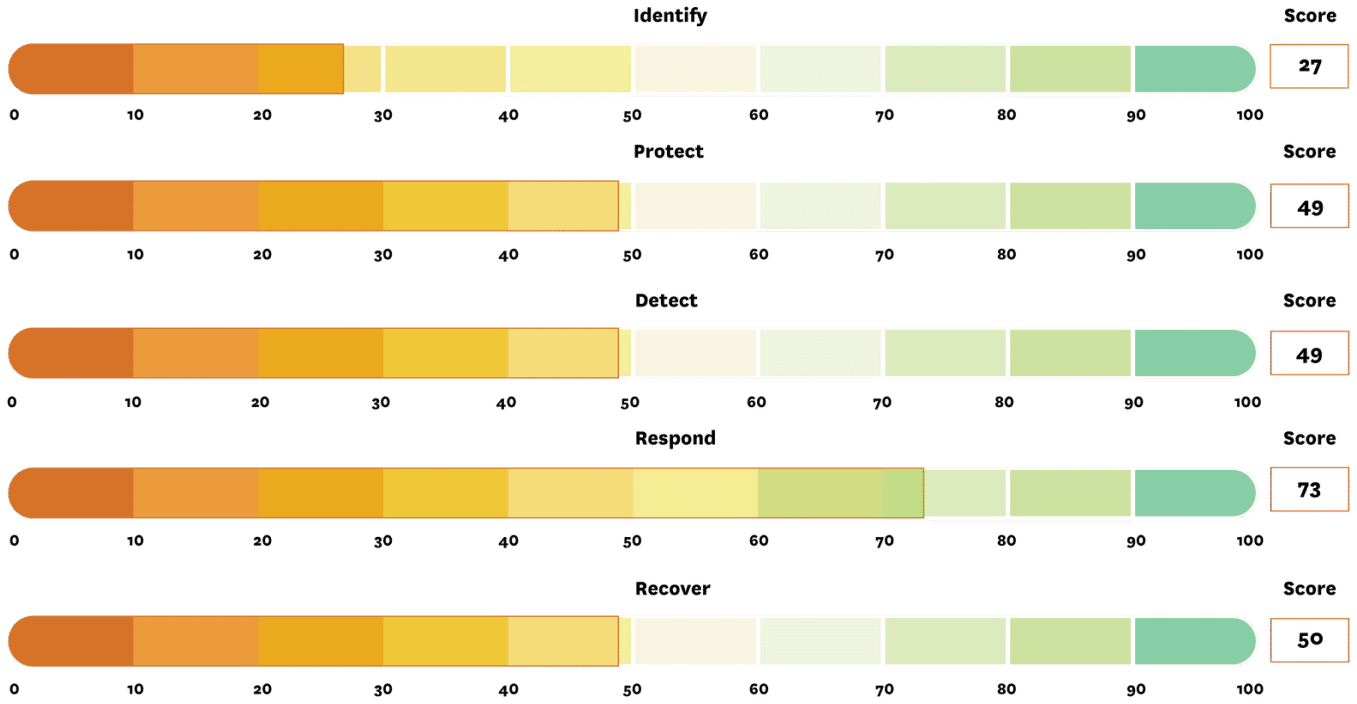
Training and awareness

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**.

Implementing a Policy Framework:

Policies **say what needs to be done**, and standards **explain how to do it**. Together, they help improve cybersecurity and keep the organisation safe.

High-performing teams **cannot thrive under old-style strict IT rules**. Today's technology leaders need **flexible, creative, and resilient governance** to keep up with fast business and tech changes.

A **policy framework** is the foundation for building **standards and procedures**:

- **Policies** define the organisation's boundaries and must align with **compliance, regulations, business strategy, and risk appetite**.
- From policies, the organisation creates **standards** that guide how people actually act and improve cybersecurity practices.

Difference between a policy and a standard	
Policy:	**Standard:**
A high-level rule or principle set by the organisation's leadership.	A detailed rule or action that supports a policy.
Guides important decisions and must be followed at all times.	Provides clear guidance on how to follow policies in practice.
Influenced by both internal goals and external factors like laws and regulations.	Creating standards requires agreement across the organisation, which can take time, but it is essential for a strong information security programme.

Aligning policy with risk appetite

Organisations use **enterprise risk management** to decide how much risk they are willing to accept—this is called their **risk appetite**.

- Some companies are **risk-averse** (low tolerance for risk).
- Others are **risk-takers** (high tolerance for risk).

A **policy framework** sets the rules for employees to follow. It's important that these policies **match the organisation's risk appetite**.

Example:
If a company has a **low tolerance for information breaches** but its policies allow weak security, this **conflicts with its risk appetite**. Employees would get **mixed messages**, leading to confusion and poor security practices.

In short: Policies should **reflect the company's risk tolerance** so everyone knows the right level of caution.

Technical Writing for IT Security Policies:

https://www.sans.org/white-papers/492

Should we measure policy effectiveness?

Why After a policy is put in place, it's **not enough to assume everyone is following it**. Organisations need to **measure policy effectiveness** to make sure policies are working as intended. This helps identify issues, make improvements, and guide future policy updates.

How to measure policy effectiveness

1. Audits:

- Audits check whether policies are being followed and are effective.
- **Compliance audits** make sure the organisation meets regulations.
- Audits are done **independently** to stay unbiased. Findings are reported to an **audit committee** (usually board members).
- Some organisations link audit results to **staff performance** or even **bonuses**.

2. Exceptions:

- Policies may allow for **some exceptions** depending on the organisation's **risk appetite**.
- During audits, auditors check if exceptions are **agreed and documented**.
- Any **unauthorised exceptions** are reported as findings and must be fixed with a remediation plan.

3. Regulatory oversight (Australia example):

- The **Australian Securities and Investments Commission (ASIC)** monitors compliance with financial reporting and audits.
- They make sure organisations have **proper policies** to manage risks and conduct due diligence.

In short:
Measuring policy effectiveness through audits and monitoring exceptions ensures that policies are **followed correctly, risks are managed, and improvements are made**. It also helps organisations stay **compliant with regulators**.

Identify measurement criteria

When measuring how well a policy is working, it's important to **know what the policy is trying to achieve**.

1. **Set clear goals** for the policy.
2. **Choose key performance indicators (KPIs)** to track progress.
3. **Establish a baseline** so you can compare future results.
4. **Regularly review the data** to see if the policy is effective and where it can improve.

Example:
If a company uses firewalls, antivirus software, and access controls, it might measure:

- How many cyber attacks were stopped
- How often incidents happen and how severe they are
- How quickly incidents are handled

These numbers help the company **improve the policy over time** as new threats appear.

In short: set goals, measure progress, track results, and make improvements.

TOOLS

Cyber threats and regulations change quickly, so **manually tracking compliance is very difficult**. While audits are useful, they are **expensive and time-consuming**. Because of this, many organisations now use **software tools** to measure compliance automatically and in real time.

Microsoft Purview Compliance Manager

This tool helps organisations **measure their compliance score** against regulations and standards.

- It works with many Microsoft systems, websites, and applications.
- It uses **real-time data** to show how compliant the organisation is.

- It includes templates for frameworks like **NIST** and **Essential Eight**.

2025 Context Note:
In 2025, Microsoft Purview Compliance Manager is still widely used. Some compliance checks are automatic, while others require organisations to provide evidence. This means the compliance score reflects both **technical controls and governance practices**.

Prisma Cloud

Prisma Cloud is used to **check compliance in cloud environments**.

- It helps organisations meet requirements such as **APRA CPS 234**.
- The goal is to reduce cyber risk by identifying vulnerabilities and threats in the cloud.

2025 Context Note:
Prisma Cloud remains widely used in 2025 and supports cloud security and compliance. However, it **supports** governance and risk management—it does not replace them.

Microsoft Azure Policy

Azure Policy helps organisations **enforce rules** on resources running in Azure.

- It checks resources automatically when they are created or changed.
- If a rule is broken, it can **block the action, raise an alert, or fix the issue**.
- A compliance dashboard shows what is compliant and what needs attention.

In short:
Modern compliance tools help organisations **monitor policies continuously, reduce manual effort, and respond faster** to risks—but they still need strong governance and oversight to be effective.

When introducing a new policy, **clear communication is very important**. If communication is poor, staff may feel confused, resistant, or distrustful, which can cause the policy to fail.

Policies work better when people **understand why the policy exists, what it means, and how it affects their work**. When everyone understands the goal, teams can work together more effectively.

Why policy documents alone aren’t enough

Policies are usually **formal and impersonal**. Simply giving staff a policy document is not very effective because:

- It may be hard to understand
- Staff may not see how it affects their role
- It may feel disconnected from daily work

Organisations should **adapt the language and communication style** to suit different teams:

- **Customer service staff** need to explain policies simply to customers
- **IT staff** need technical detail but also need to explain it to non-technical users

Use visuals to communicate better

Using **visuals** makes policies easier to understand:

- Charts, diagrams, and infographics highlight key points
- Visuals are more engaging and easier to remember
- They help non-technical staff understand complex information
- They increase buy-in and support for new policies

Visuals can also be shared easily across digital platforms, helping reach more people.

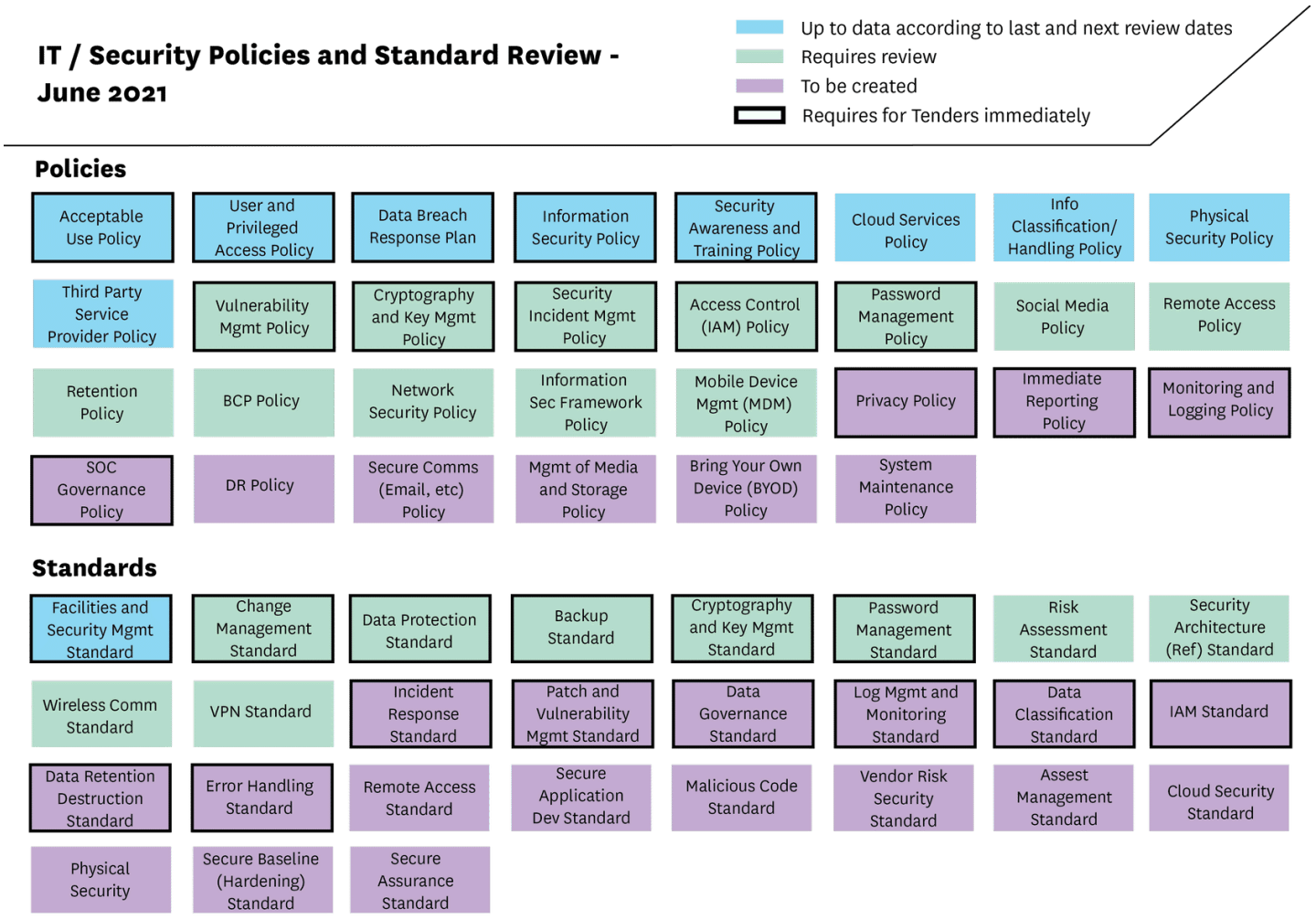
Why visuals work

One-page visuals can show:

- What policies are needed
- How they link to standards (like ISO 27001)
- Progress status using colours

This is much easier to understand than long written documents.

In short:
Good communication—especially using **simple language and visuals**—helps staff understand policies, reduces resistance, and improves successful adoption.



Cybersecurity strategies and frameworks help organisations **protect their systems and data from cyberattacks.** To work well, they must **match the organisation's business goals**. When security supports business objectives, it is easier to implement and gain **leadership support**.

Benchmarking against similar organisations is also important. It helps businesses **learn best practices**, stay up to date, and ensure their security controls meet current standards.

Change management plays a big role in success. This means keeping leaders informed through **progress updates and clear board reports**. When stakeholders understand progress, risks, and benefits, they are more likely to support the initiative and provide the right resources.

In short:
A strong cybersecurity strategy:

- Aligns with business goals
- Learns from industry peers
- Uses good change management

This helps organisations **reduce cyber risk, protect their reputation, and maintain customer trust**.

What is Governance?

Governance is basically the rules, processes, and structures that guide how a company is run. When we talk about **information security governance**, it means making sure the company protects its information in a way that also supports the business.

Even if you don't control every part of the company, understanding **how information security governance works** helps you:

- See how decisions are made
- Spot areas where processes can be more efficient
- Suggest improvements that make the business run smoother

So, in simple terms, good **governance isn't just about rules—it can also make the company work better and safer**.

Governance used to be just about rules to keep a company safe. Now, it's about **helping the company grow, adapt, and serve customers better**.

- It should let the company **change quickly** when customer needs or the market changes.
- It uses **data and technology** to predict trends and make smarter decisions.
- It makes the company **strong during crises**, so it can keep delivering value and even find new opportunities.

So basically: **good governance helps a company be flexible, customer-focused, and resilient—not just rule-following.**

How easily a company can **adapt and change** depends on **its size and how it's organized**.

- **Big companies** have lots of rules and complex governance because they operate in many countries or business areas. This can make them **slower to change**.
- **Small companies** have simpler rules and fewer layers of decision-making, so they are usually **faster and more flexible**.

In short: **the bigger and more complex the company, the harder it is to change quickly; smaller companies can adapt more easily.**

The images below describe:

Board (Top Level)

- **They oversee everything and make sure cyber risks are managed properly.**
- **They set the rules, approve budgets, and define how the company handles cyber risks.**

---

2. Committees below the Board

- **Risk Committee → Focuses on key risks and plans to handle them, including investments in cybersecurity and insurance.**
- **Audit Committee → Focuses on checking if cyber controls are working efficiently.**

---

3. Cyber Risk Governance Group

- **Led by the Risk Manager.**
- **Mission: Identify cyber risks and create plans to control or reduce them.**

- **Made up of people from Operations, IT, Data, HR, and often includes CISO, Data Protection Officer, Compliance Officer, Finance Officer.**

- **Works with Internal Audit to make sure mitigation plans are auditable (can be checked).**

---

4. Internal Audit

- **Independent check to ensure risk treatments and controls are working properly.**

---

5. Lines of Defence (3LOD model)

- **First Line → Staff from Operations, IT, Data, HR. They carry out the controls day-to-day and report risks.**

- **Second Line → Risk Manager, CISO, Data Protection Officer, Compliance Officer, Finance Officer. They monitor and guide the first line and feed info into the cyber risk governance group.**

- **Third Line → Risk Committee, Audit Committee, Cyber Risk Governance Group, Internal Audit. They oversee, review, and assure everything is working correctly.**

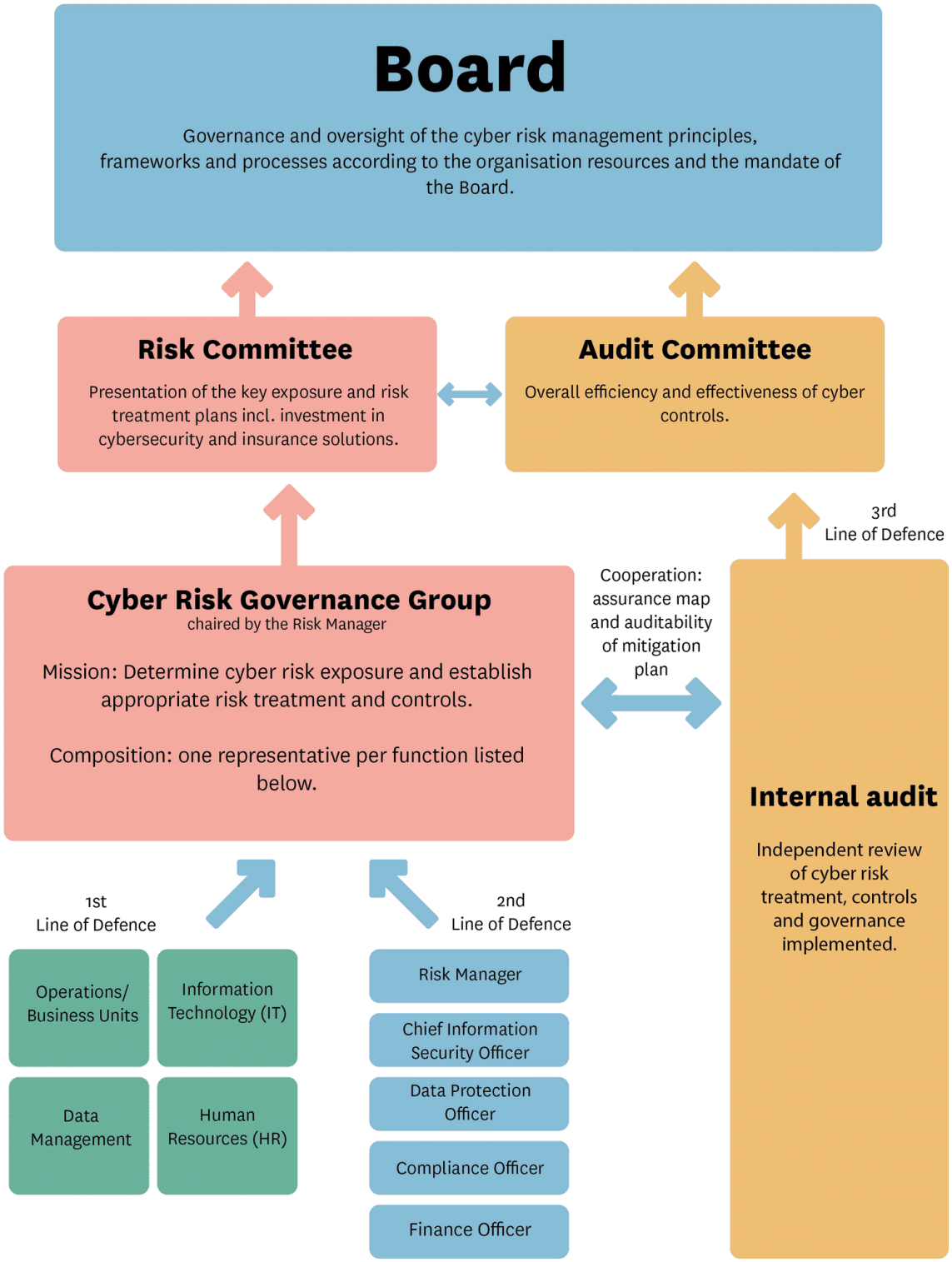
Simple analogy:

- **First line → Soldiers on the front line (doing the work).**

- **Second line → Generals planning and supervising.**

- **Third line → Inspectors and board making sure everyone follows the plan and it works.**

3LD


Board
Governance and oversight of the cyber risk management principles, frameworks and processes according to the organisation resources and the mandate of the Board.
Risk Committee
Presentation of the key exposure and risk treatment plans incl. investment in cybersecurity and insurance solutions.
Audit Committee
Overall efficiency and effectiveness of cyber controls.
Cyber Risk Governance Group
chaired by the Risk Manager
Mission: Determine cyber risk exposure and establish appropriate risk treatment and controls.
Composition: one representative per function listed below.
Cooperation: assurance map and auditability of mitigation plan
3rd Line of Defence
Internal audit
Independent review of cyber risk treatment, controls and governance implemented.
1st Line of Defence
Operations/ Business Units
Information Technology (IT)
Data Management
Human Resources (HR)
2nd Line of Defence
Risk Manager
Chief Information Security Officer
Data Protection Officer
Compliance Officer
Finance Officer

3LOD

The **Three Lines of Defence (3LOD) model** is a simple way for organisations to **manage risk clearly and effectively**. It does this by **dividing responsibilities into three layers**, so everyone knows their role and nothing is missed.

- **First Line of Defence** – People who *do the work* every day (operations, IT, business teams). They identify risks and follow controls.
- **Second Line of Defence** – People who *guide and monitor* (risk managers, compliance, CISO). They set rules, support the first line, and check risks are being managed.
- **Third Line of Defence** – People who *independently review* (internal audit, board committees). They make sure the first and second lines are working properly.

In simple terms:
3LOD helps an organisation manage risk by clearly separating who does the work, who oversees it, and who checks it.

Reporting risk:

When you communicate with the **board**, remember they are **not technical experts**. They come from backgrounds like finance, business, or management, not cybersecurity.

So when writing reports for the board:

- **Avoid technical jargon and acronyms**
- **Explain cyber issues in simple language**
- Focus on **business impact**, **risk**, and **how the risk is managed**

Instead of explaining *how* a cyberattack works, explain:

- **What could go wrong**
- **How it affects the business**
- **What is being done to reduce the risk**

In short: **talk to the board in business language, not technical language, so they can make informed decisions.**

Board Committees:

When you present cyber or risk topics to the **board**, your job is to **guide them through a decision**, step by step.

1. **Explain the problem Tell** a clear story about what's happening now, how things work, and **what the current limits or risks are**.

2. **Explain what success looks like. Show** the board the **end goal**. Explain what "bad", "good", and "great" look like so they understand what you're aiming for.

3. **Give options Present** a few realistic choices. Explain the **trade-offs** (cost, risk, time, impact on the business) so the board knows what decision they are making.

4. **Compare and recommend. Help** the board see how each option fits with the company's **strategy, budget, and capabilities so** they can choose the best option and approve funding.

telling a story that helps the board understand the problem, see the goal, compare choices, and make a decision.

A **cybersecurity audit** is done to check whether an organisation's security controls are **working properly** and protecting the business.

- It helps find **weak spots** like software flaws, network issues, or risky user behaviour.

- It checks if the organisation is **meeting laws, regulations, and industry standards**.

- It shows whether the cybersecurity strategy is **current, complete, and effective**.

By doing audits regularly, organisations can:

- Keep up with **new cyber threats**

- Improve their security over time

- Avoid **fines, legal trouble, and damage to their reputation**

In short: **cyber security audits help organisations stay secure, compliant, and prepared for cyber risks.**

Internal and External Audits:

Audits are checks that make sure an organisation is **doing things correctly and honestly**.

- **Internal audits** are done inside the organisation.
    - The audit committee decides what to check.
    - They review financial and non-financial controls and how risks are managed.
    - Their goal is to **find problems early and improve processes**.
- **External audits** are done by **outside regulators or auditors**.
    - They are required by law and set by bodies like ASIC, ATO, and DTA.
    - Their goal is to **make sure the organisation follows rules and regulations**.

Internal audits help the organisation improve. External audits make sure the organisation follows the law.

An **audit** happens in **planned steps**, and the audit schedule is usually shared at the start of the financial year so everyone knows when audits will occur.

The purpose of an audit is to **check whether an organisation's rules, controls, and compliance processes are actually working** or if they need to be improved.

Audits are **independent**, meaning they are done by people who are not responsible for the day-to-day work. This helps ensure the results are fair and unbiased.

Information security professionals are often involved because audits check **security and governance controls**, so understanding the audit process helps you know what is expected and how to prepare.

In short: **audits are planned, independent checks to make sure governance and security controls work properly and can be improved if needed.**

After an audit, a report is created that shows what is wrong and how to fix it.
The organisation must work on fixing these issues and report progress to the audit committee every three months.

If the issues are not fixed, regulators are more likely to check the organisation more closely in future audits.

In short: find issues → fix them → report progress, or face more scrutiny later.

cyber security roadmap

A cybersecurity roadmap is like a step-by-step plan for making an organisation more secure over time.

- **It shows what the organisation wants to achieve (goals and objectives)**
- **Lists the actions and projects to reach those goals**
- **Helps the organisation reduce risks and improve its cyber defences**

In short: it's a plan that guides the organisation on how to get stronger in cyber security over time.

A **cybersecurity roadmap** is a plan that shows how an organisation will **protect its IT systems, networks, and data**.

- It helps **prevent unauthorised access, misuse, or damage** to information.
- It **sets clear goals and objectives** for cyber security.
- It identifies **possible threats and weak spots**.
- It provides a **framework for managing and reducing risks**.

In short: **the roadmap is a guide to keep the organisation's digital systems and data safe while managing risks effectively.**

The **main responsibility** for making and carrying out a cybersecurity plan lies with **the organisation's management**, especially the **CISO (Chief Information Security Officer) or CSO (Chief Security Officer)**.

- They make sure the company's **IT systems and data are protected**.
- They **work with other leaders and IT teams** to create a plan that fits the company's **specific risks and needs**.

In short: **the CISO/CSO leads the effort to keep the organisation's technology and data safe, with help from management and IT staff.**

Roadmaps are generally deployed and have a 3-5 year lifecycle; however, this depends on the organisation's culture and processes.

Cybersecurity strategy vs. roadmap:

- **Cybersecurity strategy** = the **big picture plan**.
    - It answers, “What **are we trying to protect and why?”**
    - Shows the organisation’s **goals, risks, and overall approach** to cybersecurity.
- **Cybersecurity roadmap** = the **step-by-step plan**.
    - It answers, “How **and when will we achieve the strategy?”**
    - Lists **specific actions, timelines, and resources needed**.

In short:

- Strategy = **what** and **why**
- Roadmap = **how** and **when**

Together, they **help the organisation protect IT systems and data while managing risks effectively**.

What is a cybersecurity mission & vision

Think of it like this:

- **Vision** = *Where we want to go* (the long-term picture)
- **Mission** = *How we show up every day to get there*

Why they actually matter

A clear mission and vision:

- Shows leadership that you **understand the business**, not just technology

- Helps people know **why security exists**, not just what controls to follow
- Makes decisions easier when priorities clash

In short: it helps security stop being “the department that says no”.

---

2. Why involve your team?

Your team:

- Runs the systems
- Deals with incidents
- Knows what *really* breaks and what actually works

If you write the vision alone:

- It may look good on paper
- But it won’t work in reality
- And people won’t feel ownership

A simple way to engage them

You don’t need workshops or slides. Just ask questions like:

- **Who do we protect?**
  (Customers, staff, data, revenue, reputation)
- **What do we actually provide?**
  (Trust, resilience, safe systems, business continuity)
- **Why are we critical?**
  (Without us, the business can’t operate safely.)
- **What would go wrong if we didn’t exist?**
  (Breaches, downtime, fines, loss of trust)

---

3. Simple example of a cybersecurity vision & mission

Vision (future-focused)

> *To enable the organisation to grow and innovate securely, earning trust from customers, partners, and employees.*

Mission (day-to-day purpose)

> *We protect the organisation by managing cyber risk, embedding security into business processes, and enabling safe, reliable operations.*

Notice:

- No jargon
- Focus on **business, trust, and enablement**
- Security supports the business — it doesn't block it

---

4. What is a strategy canvas (explained simply)?

A **strategy canvas** is just a **big-picture map**.

Instead of starting with:

> "Here are the risks and controls."

You start with:

> "How does the business make money — and how do we protect that?"

Think of it as:

- A **conversation tool**
- A **shared planning board**
- A way to show **how security helps the business succeed**

---

5. Why this approach is better than traditional security planning

Traditional security planning:

- Lists risks
- Lists controls
- Often feels disconnected from business goals

Strategy canvas approach:

- Puts **business objectives first**
- Aligns security work to **revenue, growth, and customers**
- Helps security get involved **early**, not at the last minute

This is how you move from:

> "Security is slowing us down."
> to
> "Security helps us move faster and safer."

---

6. How cyber security supports profits (in simple terms)

Cyber security supports profit by:

- Preventing downtime (systems stay available)
- Protecting customer trust (no breaches)
- Enabling safe innovation (new products launch securely)
- Avoiding fines and reputational damage

If security is not aligned to how the organisation makes money:

- It becomes reactive
- It gets ignored
- It's seen as a cost, not a value

---

7. The big takeaway (one paragraph)

A cybersecurity mission and vision aren't about sounding impressive—they're about **showing you understand the business and your people**. By involving your team and using tools like a strategy canvas, security becomes a **business enabler**, not a blocker. This approach builds trust, improves buy-in, and helps security support growth, innovation, and profit from the start.

IdeAt its core, **organisational culture** is about *how people think, behave, and make decisions at work*.

At the deepest level, culture comes from **basic assumptions**—things people in the organisation believe are "just the way things are," often

without even realising it. These assumptions shape values and everyday behaviour. They usually relate to:

- **People** – Do we believe people are trustworthy, capable, and motivated, or do they need close control?
- **Work** – Is work seen as something to enjoy and take pride in, or just a task to get done?
- **Leadership and authority** – Are leaders expected to command, or to guide and support?
- **Change and risk** – Is change welcomed and innovation encouraged, or is stability preferred?
- **Relationships** – Is teamwork valued, or is individual performance more important?
- **Success** – Is success measured by profit, quality, ethics, customer satisfaction, or all of these?

These basic beliefs influence the organisation's **values**, which then show up in visible things like policies, behaviours, communication style, and how decisions are made.

In short:
Assumptions → Values → Behaviour → Culture

Cyber security controls only work well if **employees actually follow them**. If security rules go against how people normally think, work, or behave, they are likely to be ignored or bypassed.

Every company already has a **culture**—shared beliefs, values, and ways of working. Cybersecurity needs to **fit into that culture**, not fight against it.

That's why it's important to **involve employees** when developing the cybersecurity mission and vision. Staff understand how things really work day to day, and they can:

- Tell you what security practices will feel reasonable and acceptable
- Point out rules that may be unrealistic or disruptive
- Help shape security in a way that aligns with existing behaviours and values

When employees feel involved and heard, they are more likely to **support, accept, and follow** cybersecurity controls—making security stronger across the organisation.

Cyber security is no longer just an IT requirement — it is a **value add** for organisations.

Because of recent high-profile cyber attacks, customers are much more aware of **data privacy and security**. They want to know their personal information is safe. When an organisation clearly shows that it takes cyber security seriously, it builds **trust and confidence** with customers.

This trust can become a **competitive advantage**. Customers are more likely to choose and stay with organisations that protect their data well. On the other hand, if a company appears careless about cyber security, it may lose customers and business.

Innovative organisations now use cybersecurity to add value. For example:

- **Banks like NAB** offer cyber safety training to help their business customers protect themselves online.
- **Organisations such as AustralianSuper and Wesfarmers** include cybersecurity information as part of their safety and risk management practices.

By doing this, organisations show that cybersecurity is not just about protection — it is about **supporting customers, building trust, and strengthening the brand**.

Gap assessment

Cyber security gap assessments and **threat modelling workshops** are related, but they do different things.

A **cyber security gap assessment** looks at what security controls an organisation already has and compares them against best practices, standards, and legal requirements. The goal is to find **what is missing or weak** in the organisation's cyber security.
It helps answer questions like:

- What security controls do we have?
- What controls should we have?
- Where are the gaps or weaknesses?

This assessment is usually carried out by the **security team or auditors**. The result is a list of vulnerabilities and recommendations for improvement.

A **threat modelling workshop**, on the other hand, focuses on **how attackers could take advantage of those weaknesses**. It brings people together to think about possible cyber threats, how likely they are, and how serious the impact could be.

The results of the gap assessment are used to **guide and prioritise** the threat modelling workshop. Since the gaps show where security is weakest, these areas become the main focus when discussing potential threats.

By using both together, an organisation can:

- Understand its current cybersecurity level
- Identify where it is most vulnerable
- Focus on the most important threats
- Develop effective plans to reduce cyber risk

In short:
Gap assessment finds the weaknesses; threat modelling shows how those weaknesses could be exploited and how to fix them.

Threat **modelling** is a structured way of thinking about what could go wrong in an organisation's systems and how to prevent it. It helps organisations **identify possible cyber threats before attackers can exploit them**.

The process starts by identifying what needs to be protected, such as **data, systems, or infrastructure**. The system is then broken down into parts to understand how data moves and where weaknesses might exist. This helps identify **possible attack points**.

Threat modelling is usually done through **collaborative workshops**. People from IT, security, business, and development teams work together to:

- Identify possible threat scenarios
- Spot vulnerabilities
- Decide which threats are most serious
- Suggest ways to reduce or remove the risks

Often, the risks identified in a **cyber security gap assessment** are used to guide these workshops, helping teams focus on the most important problem areas.

Once threats are identified, they are assessed based on:

- **Likelihood** – how likely the threat is to happen
- **Impact** – how much damage it could cause

Threats can come from insiders, external attackers, or even events like system failures or natural disasters. After this assessment, **mitigation strategies** are developed. These might include adding security controls (such as access controls or firewalls) or designing systems to be more secure and resilient.

Threat modelling plays an important role in building a **cyber security roadmap**. It helps organisations:

- Prioritise security efforts and spend resources wisely
- Choose the most effective security controls
- Reduce costs by fixing issues early, before a breach occurs
- Align security initiatives with business goals

It also supports **regulatory compliance**, as many frameworks and laws (such as GDPR) expect organisations to identify and manage cyber risks proactively.

To support threat modelling, organisations often use frameworks and tools such as:

- **STRIDE** – identifies six common threat types (spoofing, tampering, information disclosure, etc.)
- **PASTA** – a step-by-step approach to analysing threats and attack scenarios
- **Threat modelling tools**, such as Microsoft's Threat Modeling Tool

In summary, **threat modelling helps organisations understand their risks, prevent security issues early, and build stronger, more secure systems that support business objectives**.

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

To run a successful **threat modelling workshop**, you need good planning and clear steps so everyone knows what to focus on and what to do next.

1. **Define the scope Decide** what system, application, or process you are looking at and what assets need protection (such as data or systems). This keeps the workshop focused on what matters most.
2. **Identify stakeholders Invite** the right people, such as IT, security, developers, and business representatives. Make sure they are available so all key perspectives are included.
3. **Choose a facilitator**
   Select someone experienced in threat modelling to lead the session. The facilitator keeps discussions on track, encourages everyone to contribute, and manages time effectively.
4. **Choose a methodologyPick** a threat modelling method that suits your organisation, such as **STRIDE** or **PASTA**. This gives the workshop a clear structure.
5. **Prepare materials**
   Provide templates, diagrams, or guidelines ahead of time so participants can come prepared and understand what will be discussed.
6. **Run the workshopDuring** the session, work through the threat modelling steps together. Encourage open discussion and teamwork, and record all identified threats and

weaknesses.

7. **Prioritise threats**
   Rank the threats based on how likely they are and how much damage they could cause. This helps focus on the most important risks first.

8. **Create a mitigation plan Decide** how to address the highest risks. Assign actions, timelines, and owners so it's clear who is responsible for what.

9. **Follow up After** the workshop, check that the agreed actions are being implemented and resolve any remaining issues.

In short, a well-run threat modelling workshop helps teams **identify risks, agree on priorities, and take clear actions to improve security**.