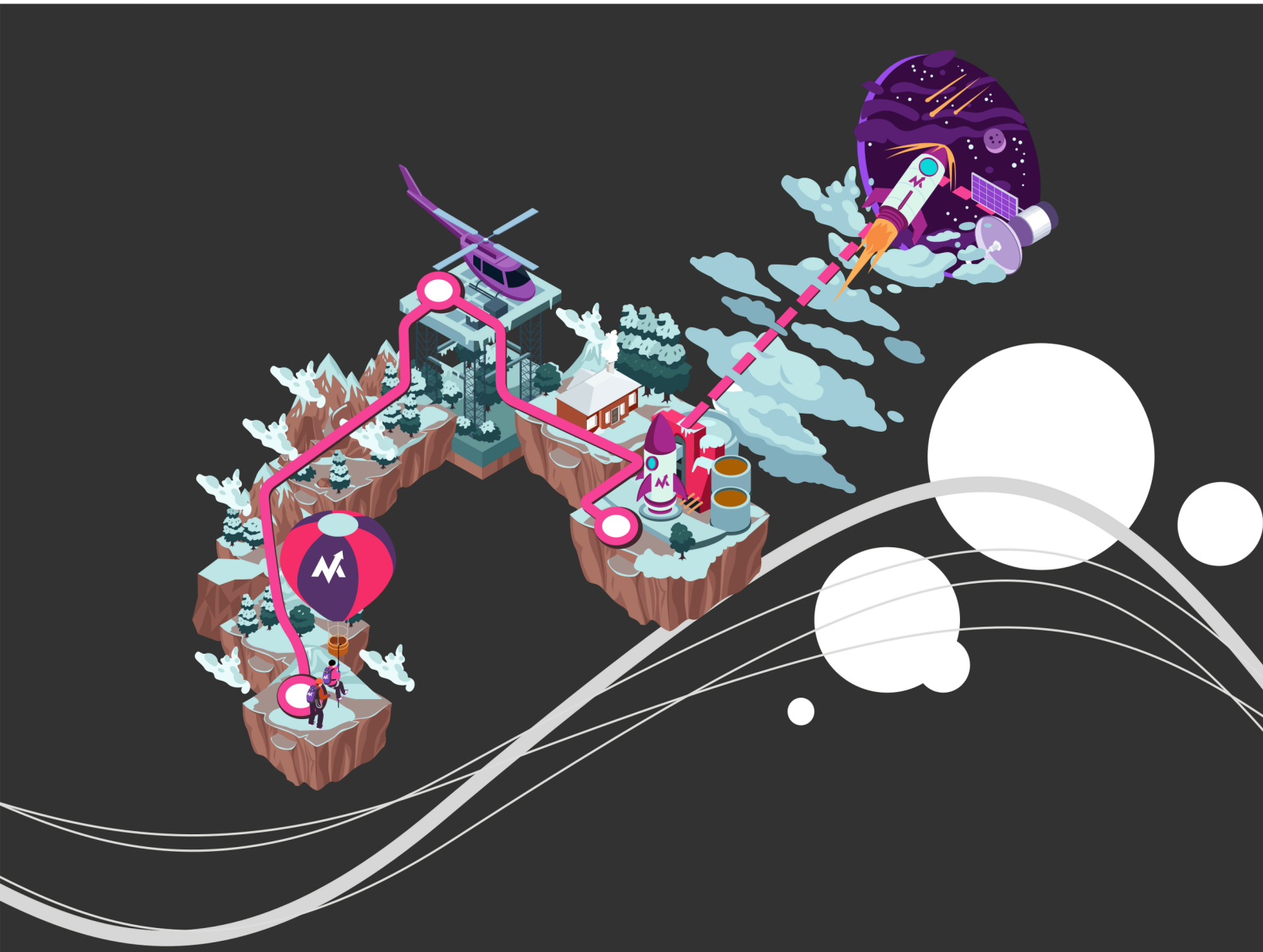
MyCISO

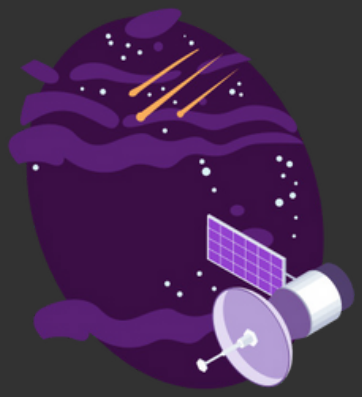
SECURITY
MANAGEMENT
SIMPLIFIED



THE ULTIMATE GUIDE TO SUPPLY CHAIN SECURITY MANAGEMENT

According to PwC's 2023 Digital Trust Insights Survey[1], third parties are one of the top threat vectors that Australian organisations are least prepared to address. In fact, nearly half (46 per cent) of Australian organisations believe third-party suppliers are one of the top pathways adversaries would use to gain access to business systems.

Cybercriminals increasingly target third-party suppliers for a number of reasons. Unfortunately, suppliers both large and small represent a risk to your business, especially if they have privileged access, hold or have access to your sensitive data. Whilst larger companies may have resources for more sophisticated security controls, their size can increase complexity and lead to gaps emerging in their security posture. Asking the right questions of your suppliers will uncover whether your organisation would be at risk, if the supplier was involved in an incident.



When a cybercriminal compromises a third-party supplier, they can also potentially gain access to multiple clients, making the attack more lucrative because they are able to steal sensitive information, credentials, or intellectual property from several organisations - multiplying the impact of the attack.

Attacking an organisation through their third-party supplier can be lucrative for cybercriminals. Such an attack can cause significant disruption to both the supplier and their customers, leading to production delays, financial losses, and reputational damage – all things organisations may pay high ransoms to avoid.

LONG, UNRELIABLE PROCESSES

The challenge is that many organisations have limited visibility into the security practices of their third-party suppliers. This lack of oversight makes it difficult to assess and mitigate the risks associated with working with these suppliers, creating vulnerabilities that cybercriminals can exploit.

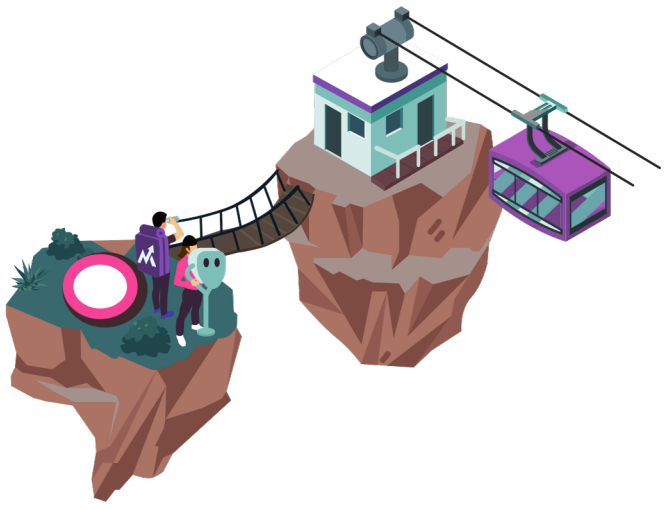
This is complicated further by the fact that the third-party risk management (TPRM) market for these solutions is quite fragmented, resulting in companies having to make trade-offs while searching for an ideal solution.

According to Gartner's Market Guide for Third-Party Risk Management Solutions[2], most organisations end up settling for a combination of solutions and risk domain insights, which are used by various teams across enterprise risk, compliance, procurement, supply chain, IT, cybersecurity, and environmental & social governance (ESG).

For years business leaders have been attempting to solve this problem, using a myriad of tools from spreadsheets to isolated assessment tools that deliver an unfulfilling experience for both the cyber leader and the third-party.

The result? Cyber leaders spend hours analysing each assessment to check if it meets the benchmark, get drawn into long email dialogues looking for additional information, and end up losing track of expired security assessments or re-assessment requirements. Suppliers operate like a trojan horse for a business, being allowed to operate within trusted zones, whilst the security posture for the organisation drifts outside of an acceptable state. It's no wonder gaps are emerging, weakening supply chains and exposing businesses to risks.

To address these challenges and protect their networks, organisations need to prioritise third-party risk management, conduct regular security assessments of their suppliers, and implement strong security controls and monitoring across their supply chain.



EIGHT STEPS TO SECURING YOUR CYBER SUPPLY CHAIN

If a supplier, manufacturer, distributor, or retailer is involved in products or services used by an organisation (in other words, any business that forms part of a supply chain), there will be a supply chain risk originating from it.

Similarly, an organisation will transfer any supply chain risk they hold to their customers. The good news is that there are steps organisations can take to protect their supply chains.

These are:

1. Identify the supply chain.
2. Organise and define supplier criticality levels.
3. Determine which security questions you wish to assess, by criticality level.
4. Create a baseline of discovery questions.
5. Determine cybersecurity expectations (pass or fail rates).
6. Determine frequency of re-assessment (if required).
7. Determine whether external validation is required.
8. Implement a management system to collect assessments and manage supply dialogue.

Performing these steps will vary from business to business. In some cases, the process will be fairly simplistic, particularly if only a small number of suppliers need to be assessed. However, where there are a range of criticality levels and deep and comprehensive assessments are required, the process can become highly advanced (and time-consuming).

1. IDENTIFY YOUR SUPPLIERS

Map out all the suppliers and third-party relationships for your organisation. This should include both IT Infrastructure (software and hardware) providers and non-IT suppliers, such as business services, including legal, accounting and marketing services.

There can be a surprisingly high number of suppliers in your supply chain. A good way to find out who your suppliers are is to speak to the finance department, who should already have a list of approved or expected suppliers.

You're going to need to create a list of your suppliers detailing as much information as practicably possible, including:

1. Legal entity name and trading name.
2. Office address and phone number.
3. Contact name and email address.
4. Current annual spend.
5. Supplier internal owner – this should be the primary point of contact from your organisation that works with this supplier.

2. ORGANISE AND DEFINE SUPPLIER CRITICALITY LEVELS

Most organisations use three levels of criticality: low, medium, and high. There are a number of factors that impact criticality. These include:

Contract value: suppliers with larger contracts are probably providing more business-critical services to your organisation, which means a security breach to that organisation could directly impact you. The higher a contract, the higher the criticality rating.

Data volume: the personally identifiable information (PII) of one person is far less valuable than the PII of thousands of people. A cybercriminal is far more likely to target suppliers who hold bigger PII repositories.

Data sensitivity: some data is more critical than others. For example, customer data and government data that is subject to regulations or customer contract obligations could make the supplier more critical (and once again, more valuable as a target).

Physical access level: does the supplier have physical access to your sites or offices, where sensitive data is held?

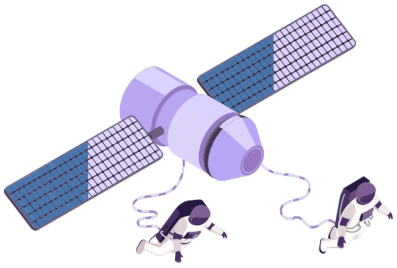
System access level: does the supplier have access to systems that hold sensitive data? Does the supplier have privileged credentials?

Mission criticality: does the supplier provide a product or service that could become unavailable during an incident?

Determining supplier criticality into low, medium and high can be done in several ways, depending on your organisation's risk appetite. It's a good idea to understand the business impact of different incident types when considering which criticality level to place a supplier.

A simple approach can include creating a scoring matrix as follows:

Where 0 is NA, 1 is low, 2 is medium and 3 is high, a score can be placed in each cell to create a cumulative supplier score.

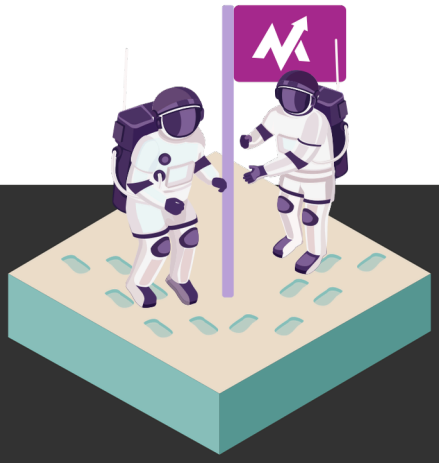


	Contract value	Data volume	Data sensitivity	Physical access	System access	Mission criticality	Total
Supplier 1	0	0	1	0	1	0	2
Supplier 2	2	2	1	0	3	1	8
Supplier 3	3	2	3	2	2	1	13

Each supplier would have a cumulative score and you should set the thresholds according to your risk level.

- A score of 0-2 = NA
- A score of 3-5 = low criticality
- A score between 6-8 = medium criticality
- A score between 9-15 = high criticality

Another consideration, regardless of score, is ensuring that any scores of 3 could be deemed a high criticality supplier, irrespective of the other scores.



3. DETERMINE WHICH SECURITY CONTROLS OR FRAMEWORKS YOU WISH TO ASSESS

Carefully analyse your organisation's specific needs and industry requirements. Here are a few areas to focus on:

Understand your organisation's risk appetite: review your risk tolerance and overall risk management strategy. For example, if risk of critical system downtime is intolerable for your business, then the questions need to identify the supplier's readiness to mitigate this type of incident.

Review industry-specific regulations and standards: understand the regulations and industry standards that apply to your organisation, as compliance with these may dictate the risk domains you should be focusing on.

Assess historical performance and incidents: review past security incidents and performance issues involving your suppliers to identify recurring patterns or vulnerabilities. This information can help you prioritise risk domains that may require more attention during assessments.

Since you have now divided your suppliers into three criticality levels, you need to determine to what degree you will assess each supplier criticality level. For a low criticality, this could be very basic and incorporate the essential controls only. However, for a high criticality, you might require the supplier to conform to a similar standard of security as your own organisation and therefore assess against the full ISO 27001 standard or NIST framework.

Larger frameworks will take longer for the supplier to complete, and longer for you to review properly. Right-sizing the assessment for the risk level associated with the products or services being provided by the supplier is important. It's also worth noting that some suppliers (e.g. a stationary provider) may be unwilling to complete a comprehensive assessment, given the effort involved in comparison to the contract value.

4. CREATE A BASELINE OF DISCOVERY QUESTIONS FOR EACH SUPPLIER CRITICALITY LEVEL

These questions should speak directly to the criticality of each supplier. The goal is to gain a better understanding of how the supplier services your business so that you can determine their criticality.

You may have an idea before you begin, so keep yourself open to making adjustments to criticality levels based on what you learn. The criticality of suppliers may also change over time.

Questions to ask could include:

- what types of data do you hold?
- in which jurisdictions is the data held?
- how long have you been a supplier to us?
- do you conform to any industry recognised security standards?
- do you hold any current organisation certifications for security and privacy (e.g. ISO 27001)?

5. SET CYBERSECURITY EXPECTATIONS FOR EACH CRITICALITY

Once you have selected the security frameworks and control questions to assess with, it's important to determine the pass/fail levels for each framework and specific questions. This can be set at both a framework level (e.g. a score average of 2.5 out of 5), or you can set control or security domain specific minimum scores (e.g. business continuity and disaster recovery at a minimum score of 3).

This will need to be done for each criticality level, establishing specific expectations that are proportionate to the risks involved. Higher criticality levels will typically require more stringent security controls and closer monitoring.

For example:
Low criticality: An average score of 1.5 is acceptable for basic security controls, such as antivirus software, firewalls, and regular software updates.

Medium criticality: An average score of 2 for the more basic controls, plus some advanced security measures, such as encryption, multifactor authentication, and regular vulnerability assessments.

High criticality: A security standard compliant average score of 3 should be maintained for all controls, including the more stringent controls, such as continuous monitoring, intrusion detection systems, and frequent security audits.

You should also consider whether you require evidence, such as documents and screenshots, in your audit. This can be useful to validate whether the given score can be confirmed with evidence.

When analysing the assessment results, it's unlikely anyone will ever have a 'perfect' score. However, knowing where each supplier has strengths and weaknesses can be critical to protecting your own security posture.

Once you have determined your expectations, clearly outline them for each criticality level in your contracts with suppliers. Make sure suppliers understand their responsibilities and the consequences of non-compliance, such as penalties or even the termination of the contract. This may not be possible for all existing suppliers, or suppliers where contracts are not negotiable.

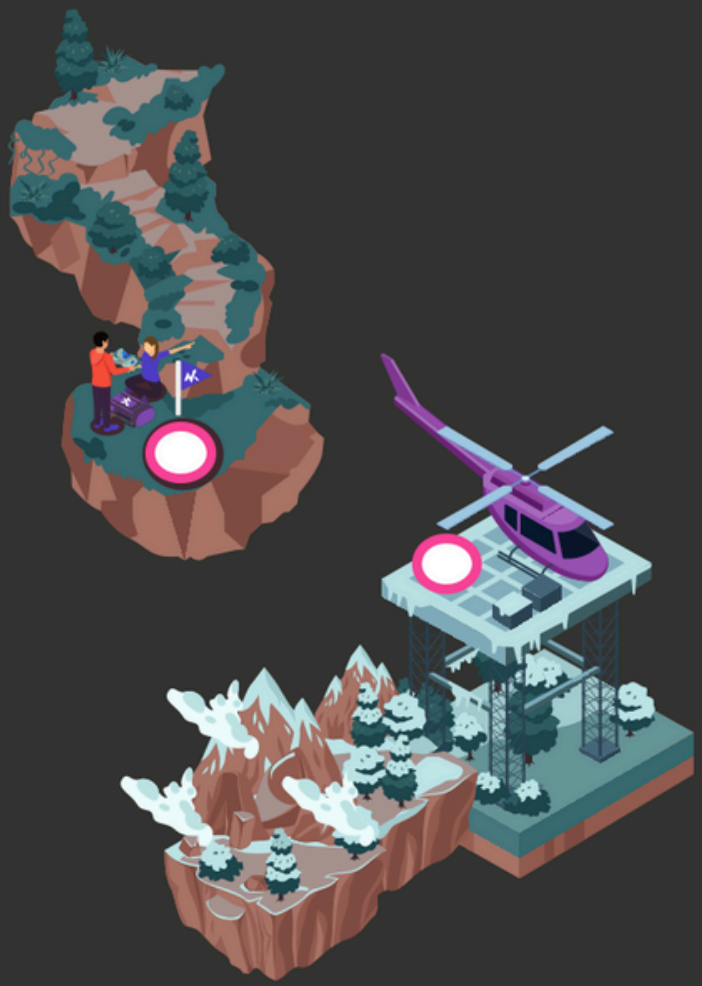
6. DETERMINE FREQUENCY OF RE-ASSESSMENT

Determining the frequency of assessing your supply chain depends on several factors, such as the criticality of the suppliers, the sensitivity of the data involved, and the ever-changing threat landscape.

A good rule of thumb is to conduct assessments on the anniversary of contract renewals, such as every one to three years, or more regularly for high criticality suppliers or those handling sensitive data.

7. DETERMINE WHETHER YOU NEED EXTERNAL VALIDATION

External validation can provide a benchmark against industry best practices and helps you understand how your organisation's cybersecurity posture compares to others in your sector. This information can be valuable for identifying areas of improvement and prioritising risk mitigation efforts.



Best practice methods for these can include:

External security audits aligned to frameworks

An external audit provides the most comprehensive view of an organisation's security maturity and showcasing that a framework such as ISO 27001, SOC-2, or NIST was performed, provides a meaningful benchmark that the organisation adheres to a robust level of security. It's important to check the scope of the assessment to make sure it includes the infrastructure used to deliver your products or services.

External and internal penetration tests

Organisations should be performing periodic penetration tests of their environment, especially servers that are mission critical or contain customer data. It's a good idea to request the certificates from the assessments, to show that the vulnerabilities found were retested to validate they had been remediated.

External automated monitoring services

These tend to provide less relevant or accurate information. These services will typically require the domain URL and IP address, which is then used by an external server to scan and investigate threat intelligence to determine any indicators of weakness. However, this approach can also contain false positives or lack context, and falsely flag a domain or IP as having weak security. Use with caution.

8. IMPLEMENT A MANAGEMENT SYSTEM TO COLLECT ASSESSMENTS AND MANAGE SUPPLIER DIALOGUE

To implement a management system for collecting assessments and managing supply dialogue, follow these steps:

Choose a platform: select a suitable platform or tool, such as MyCISO Suppliers, that allows you to easily centralise assessment data and facilitate communication with suppliers.

Define processes and workflows: establish clear processes and workflows for assessment collection, review, and follow-up, ensuring consistency and efficiency in your risk management efforts.

Assign roles and responsibilities: determine internal team members and set expectations for managing supplier assessments and communication.

Monitor and refine: regularly review the effectiveness of your management system and make adjustments as needed to optimise its performance and usability.

Below is the typical setup and ongoing management process for supplier risk management.

Identify and classify suppliers

- By geography
- By contract value
- By access levels
- By business impact

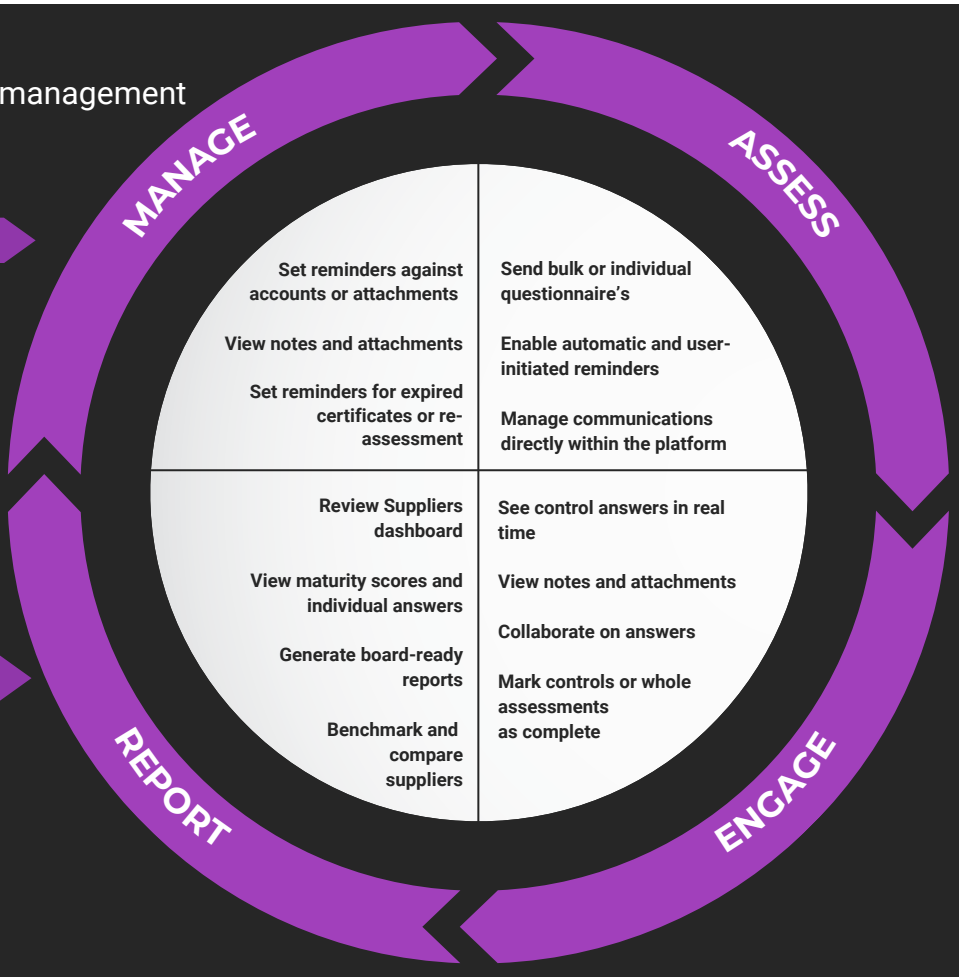
↓

Organise into criticality levels

Define assessment

Define an assessment for each criticality level, considering:

- Custom questions to ask
- Security framework to use
- Appropriate pass rate



DE-RISK YOUR SUPPLY CHAIN

Like to see a demo? Speak to the team at MyCISO about de-risking your supply chain security management cost-effectively and with ease.

sales@myciso.co +61 2 9165 8080

CONTACT US TODAY ←