MyCISO Service Descriptions

Published Date: 23rd October 2025

These service descriptions provide a detailed descriptions of the features and functionality included in the service provided and form part of the Agreement between the parties. Features will change from time to time, with the objective to continually improve the service offerings without materially degrading the overall service offering and this document will be updated accordingly. The document version will be delineated by the number in the footer of each page. This document together with release notes published on a periodic basis, will communicate the changes to the platform.

Changes to the platform will be communicated via email (to platform users) and accessible in the release notes, found at:

https://comms.myciso.co/s/article/MyCISO-Releases

Table of Contents

1. MyCISO Platform

The MyCISO platform is designed to help IT and Security leaders, or their Security Provider simplify the management of their security program. There are four primary modules, with an overlay of an external vulnerability scanner to augment your posture discovery. The four primary modules are;

- **Assess**: Our flagship product with allows the user to choose a cyber security framework, assess their maturity against the controls within the framework, and produce a series of reports. A gap assessment, a risk assessment, a cyber improvement strategy report, and a series of board reports.
- **Suppliers**: Take the functionality of the Assess module and point that focus on your supply chain to improve you third party risk management.
- **Culture**: Provides the ability to build a cyber awareness and resilience culture in your organisation via online training, phishing attack simulation, and a gamified approach to improving the resilience to scams and social engineering within your employees.
- **Incidents:** An incident management platform that allows you to build your playbooks in-app and manage your incident response in a centralised location, complete with clear reporting and PIR.
- **Metrics:** Gather outcome-driven metrics to measure the effectiveness of your cyber security program.
- **Vulnerabilities**: is not technically a module in itself, it provides an integration with Security Scorecard and Microsoft Secure Score to augment your cyber posture discovery by providing over 600 points of reference mapped into the MyCISO control database. Vulnerabilities is also used to assess third party risk.
- **Risks:** Identify, assess, and manage organizational risks.
- **Assets:** Track and protect critical business assets.
- **Toolbox:** Your Swiss-army knife of tools and templates.
- **Reporting:** Instantly generate powerful, board-ready security reports.
- **PrecogAI**: Advanced predictive AI engine for proactive security.
- **API & Integrations**: Sync seamlessly with 550+ apps and tools.
- **Group Accounts**: Manage subsidiaries with integrated, roll-up reporting.
- **Files & Evidence**: Store, organize, and track compliance evidence securely.

Since MyCISO is a SaaS platform, the features of the platform will be amended from time to time, which in turn this document will be updated accordingly.

Feature	Description
Account Management	1. Primary account management and user details 2. Change/contact details 3. Authentication method – SMS/Authenticator app 4. Applied user limits 5. Subscribed products a. Culture b. Assess i. Vulnerabilities

Feature	Description
	c. Suppliers i. Vulnerabilities d. Vulnerabilities 6. Customisable company logo 7. Additional admin account creation 8. Admin user permission levels
Company Profile	1. Country of operation and time zone 2. IT and security roles within the organisation 3. Company headcount, annual turnover, risk impact level, cyber security budget, and industry selectors 4. Sensitive information selectors 5. Security driver selectors
Users	1. Single user, bulk user, and Azure AD connect options 2. User tag management a. Custom tag edit/add b. User tag quiz selector and customisation c. Azure AD tag mapping 3. Deactivate/Activate/Delete users en-masse
Notification centre	1. Review all notifications on a user-by-user level 2. Set notification preferences between no contact, weekly update and real-time. 3. Pin notifications to the list 4. Snooze notifications for 7 days 5. Dismiss notifications 6. Bulk edit multiple notifications at once 7. Filter notifications by type or module
File Store	1. Repository for generated reports from both the Assess, Culture and Supplier modules. 2. Generate new report – Dynamic report generation based on frameworks completed and subscribed products. Schedule recurring reports.

2. MyCISO Provider account

MyCISO provider accounts are designed to be used by GRC consulting partners, Managed Services Providers, and other professional organisations wanting to utilise the MyCISO platform on behalf of their customers. The provider accounts can be used to create client accounts or groups of client accounts linked to the “parent” provider account, to summarise activity and manage engagements.

Feature	Description
Account Management	1. Primary account management and user details 2. Change/contact details 3. Authentication method – SMS/Authenticator app 4. Customisable company logo 5. Additional admin account creation 6. Admin user permission levels 7. Account login logs
Dashboard	1. Maturity RAG status 2. Current and last month averaged overall status 3. Upcoming client account renewal notifications 4. Dashboard summary of all client and group accounts a. Inactive account summary b. Sort via account type, risk rating, control or culture score. c. View client account summary cards including user counts and subscribed products d. Summarise active frameworks, questions answered, deficient controls, Assess maturity, risk rating, Culture maturity, last login. 5. Login to any attached accounts 6. Export dashboard data 7. Export filtered dashboard data 8. Add a new Group account 9. Add a new Client account
File Store	1. Generate or schedule a Strategic Security Review report

3. MyCISO Group account

MyCISO group accounts are designed to administer multiple client accounts under a group account. The intended use is for holding companies that want to group multiple businesses under one parent account, or for larger organisations who want to manage sections of their business separately.

Feature	Description
Account Management	1. Primary account management and user details 2. Change/contact details 3. Authentication method – SMS/Authenticator app 4. Customisable company logo 5. Additional admin account creation 6. Admin user permission levels

Feature	Description
	7. Account login logs
Dashboard	1. Maturity RAG status 2. Current and last month averaged overall status 3. Upcoming client account renewal notifications 4. Dashboard summary of all client and group accounts a. Inactive account summary b. Sort via account type, risk rating, control or culture score. c. Summarise active frameworks, questions answered, deficient controls, Assess maturity, risk rating, Culture maturity, last login. d. Login to all attached Client accounts e. Export dashboard data f. Export filtered dashboard data
Controls	1. Sync client accounts – Select from the attached Client accounts to the Group account that you wish to take ownership of the selected controls. 2. Search entire MyCISO control library via control ID, control name, domain name 3. View only Sync'd control toggle 4. Take ownership of controls: a. Set maturity for a control, sync'd Client accounts will inherit this maturity b. Add notes to controls c. Add related links to controls d. N/A control e. De-Sync control
File store	1. View reports saved by each of the individual attached Client accounts 2. Create or schedule a Group account report to be generated

4. MyCISO Client account

A MyCISO Client Account operates as a fully functional, standalone account with access to all platform features and capabilities. Designed to be managed under a Group Account, it provides flexibility for organisations to administer individual business units or subsidiaries independently while retaining centralised oversight at the group level.

- Does not include any vulnerability scans on its own.

5. MyCISO Assess

The Assess module allows the Security Consultant to gain business context around an organisation's sensitive data, their drivers for security, conduct a cyber control and risk assessments, and produce consultant-grade reporting. The Assess platform is designed to achieve every step in the simplest way possible, providing quick wins to customers. Whether you want to understand the best security framework for your business, assess your maturity or create your first strategy, MyCISO gives you the power to do that very easily.

- **Controls -** MyCISO has reviewed over 1200 cyber security controls and mapped these against various frameworks (e.g. NIST, ISO27001, etc). The Controls Assessment measures your maturity level per control on a scale of 0-5. Each maturity level is succinctly explained so you can move through your Controls Assessment with ease.
- **Risks** - We have identified the 15 most common risk scenarios and ranked their likelihood using your control maturity against the framework you are assessing against. The MyCISO user needs to determine an impact level for each scenario presented which results in a Risk Rating for each of the 15 risk scenarios.
- **Strategy** - This score, combined with the Control Assessment, helps us to identify the priorities for which you should deploy or improve your Control coverage.
- **Vulnerabilities** – via integration with a third-party, MyCISO can provide observed vulnerabilities linked to an organisation's primary domain and any discovered FQDNs (fully qualified domain names) linked to that primary domain. There are approximately 230 points of mapping between potential vulnerabilities and MyCISO cyber controls.

The controls assessment and risk assessment sections include their own discreet and comprehensive reports that provide a summary and insights into your organisation's controls and risk status.

The Security Improvement Strategy combines those inputs alongside your business context and maturity goals to create a security strategy that prioritises the initiatives that will drive the greatest risk reduction possible. The downloadable security strategy report provides a comprehensive summary of your inputs before applying the MyCISO algorithm to build your improvement roadmap that is Board signoff ready.

Assess your security and risk posture and create a Security Improvement Strategy aligned to risk reduction. The Assess module consists of five key features.

- Framework Selector
- Control Maturity Assessment
- Risk Assessment
- Vulnerabilties
- Security Improvement Strategy Builder
- Consultant-grade reports (without consultants!)

Feature	Description
Dashboard	1. Set target maturity levels 2. View risk summary – Average value and detail risk heat map modal

Feature	Description
	3. Filter review current framework controls including – CTUI score, Responsible staff member, Last updated, Current maturity, Target maturity, Deployment effort. 4. Control detail modal 5. Export data – All data or Filtered data
Framework Selector	1. Access to any of the available cyber security frameworks, i.e. a. MyCISO Getting Started b. MyCISO Intermediate c. NIST CSF 1.1 d. NIST CSF v2.0 e. ISO/IEC 27001:2013 f. ISO/IEC 27002:2013 g. ISO/IEC 27001/2:2013 h. ISO/IEC 27001:2022 i. ISO/IEC 27002:2022 j. ISO/IEC 27001/2:2022 Combined k. Prudential Standard CPS-234 l. APRA CPS 230 m. CIS-18 v8.0 n. Victorian Protective Data Security Standards o. Australian Privacy Principles p. ACSC Essential 8 q. SA CSF (South Australia Cyber Security Framework) r. ASD ISM Mapping 2024 s. AICPA SOC 2 t. General Data Protection Regulation (GDPR) u. Third Party Risk Management (MyCISO) v. PCI-DSS v3.2 w. PCI-DSS v4.0 x. PCIDSS v4.0 SAQ A y. PCIDSS v4.0 SAQ A-EP z. PCIDSS v4.0 SAQ B aa. PCIDSS v4.0 SAQ B-IP bb. PCIDSS v4.0 SAQ C cc. PCIDSS v4.0 SAQ C-VT dd. PCIDSS v4.0 SAQ D Merchant ee. PCIDSS v4.0 SAQ D Service Provider ff. PCIDSS v4.0 SAQ P2PE

Feature	Description
	gg. MyCISO Zero Trust hh. PSPF (Protective Security Policy Framework) ii. AESCSF v2 (Australian Energy Sector Cyber Security Framework) jj. AESCSF v1 (Australian Energy Sector Cyber Security Framework) kk. Cyber Insurance Readiness ll. SMB1001 mm. NIST AI Risk Management Framework nn. NIST Privacy Framework oo. NIST for SMB pp. Monetary Authority of Singapore –TRM 2. Up sync - Sync the maturity of the controls in that framework **up to** the master framework 3. Down sync – Sync the maturity of the controls in the master framework **down to** the controls in that framework 4. Start new/Import answers – Start the framework assessment with blank answers or import previously assessed control maturity from the master framework. 5. Maturity Descriptions - Replace the maturity descriptions for all frameworks standardised descriptions or create your own descriptions that match your organisations security language. 6. Accept scan maturity – after a scan license has been applied to a domain under Vulnerability Licensing, the scan result can be applied to your current control maturities to augment your own assessment. 7. View only started assessments
Controls	1. Filter controls based on Maturity, N/A, “Assigned to me”, Unanswered, and External Scan 2. Access to the maturity of the controls defined within the active framework 3. Assign control to active admin or staff member 4. View detailed control information including framework mapping via the “More Information” button. 5. Add notes and links to controls via the “Control Detail” button a. N/A the control 6. If framework includes compliance points these will also be displayed
Risks	1. Access to the 15 risk scenarios 2. Up sync/Down sync risks across frameworks 3. View risk scenarios “Assigned to me” 4. Review your scenario control effectiveness, based on your control maturity 5. Review the likelihood and impact risk sliders 6. Assign risk to active admin or staff member

Feature	Description
	7. View/amend control relevancy to each risk
Vulnerabilities	**External Vulnerabilities** 1. Sort the results on the page via domain name, scan level, or issue. 2. Review the vulnerability scan results per scanned domain. a. Level 3 scan provides: i. Top level score out of 100 plus A - F grade ii. 10 Factor scores out of 100 iii. Full 200+ vulnerability scan with results broken down into severity b. Level 2 scan provides: i. Top level score out of 100 plus A - F grade ii. 10 Factor scores out of 100 c. Level 1 scans provides: i. Top level score out of 100 plus A - F grade **Internal Vulnerabilities** 3. VULNERABILITIES Mk2: We have revamped the vulnerabilities feature combining the licensing and results screen into a single view. With a new layout it has never been easier so digest such a large amount of data. Adding to the previous external internet facing vulnerabilities we have the new internal vulnerability scan. All of this takes our vulnerability scanning for the ASSESS module to new heights. Some further detail on the changes: a. External scan NEW ADDITION: Level 4 scans are now available. These deliver detailed and contextual insights like Level 3 with the added benefit of specific remediation recommendations to support resolution. All exportable into CSV format for sharing. b. Internal scan: NEW ADDITION introduces another 300+ data points gathered across your internal Microsoft infrastructure. Mapped into the MyCISO control database for even smarter auto maturity recommendations and constant monitoring. c. PrecogAI Framework: Combining the control mappings for both internal and internal vulnerabilities we have created a comprehensive technical framework which can auto populate plus continually sync as vulnerabilities change over time. 4.
Vulnerability Licensing	1. 1 x level 2 scan included with Assess 2. Filter domains via scan level or status 3. Export your license summary 4. Add domains to be potentially licensed for scanning 5. Apply scan scores to your framework assessment (to augment the self-assessment with discovered vulnerabilities) 6. Promote a validated domain to be scanned at level 2 or 3

Feature	Description
File Store	1. Repository for generated reports from both the Assess, Supplier and Culture modules. 2. Generate new report – Dynamic report generation based on frameworks completed and subscribed products. 3. Schedule recurring reports.

6. MyCISO Culture

Security Culture provides an automated and streamlined, yet integrated approach to raising awareness of the common cyber-risks relevant to your staff. The MyCISO culture platform consists of the following key features.

- Strategy Builder
- E-Learning
- Automated Attack Simulation
- Staff engagement assets
- Games
- Reports & Dashboards

Feature	Description
Dashboard	1. The My Culture Dashboard displays multiple widgets illustrating the current maturity rating of the organisation against multiple metrics, including cyber awareness training and phishing campaigns 2. Filter by date range and or activity type
Strategy	1. Generate a new culture strategy – Define duration, Start date, Activity type, topics 2. Add new individual activities 3. Activate LMS mode 4. Activate catch up mode 5. Hide delivered activity 6. Generate strategy timeline 7. Duplicate, remove, edit, future strategy activity items 8. Mass edit tags tied to strategy items
E-Learning Modules	1. Video training: a. Animated training videos – 9 episodes b. Detective training videos – 8 episodes c. Threat series training videos – 10 episodes d. Role specific series videos – 1 episode
Games	1. Training games: a. Spot the difference – 3 rounds b. Two truths 1 lie quiz game – 1 round
Staff Engagement Assets	1. Posters 2. Newsletters 3. Screen savers & Digital signage 4. Webinar 5. Booklet

Feature	Description
Attack Simulation	1. Preview/Configure the attack simulation service. a. Whitelist “attack source” domains b. Running test delivery c. Configuring a campaign schedule d. Review, add, edit users e. Review campaign results
Reports	1. Reporting by topic and period on: a. Training videos b. Training games c. Attack simulation d. Awareness summary 2. Filter reporting data by tag and status 2. Export report data in CSV
Users	1. Single user, bulk user, and Azure AD connect options 2. User tag management a. Custom tag edit/add b. User tag quiz selector and customisation c. Azure AD tag mapping 3. Deactivate/Activate/Delete users en-masse
File Store	1. Repository for generated reports from both the Assess, Culture and Supplier modules. 2. Generate new report – Dynamic report generation based on frameworks completed and subscribed products. Schedule recurring reports.

7. MyCISO Suppliers

MyCISO Suppliers provides a streamlined way to address your third-party risk management. This module allows you to add organisations in your supply chain, rank them by criticality to your organisation, provide them with a cyber framework assessment along with custom questions.

The response to these assessments is managed through a dashboard, and can provide detailed reporting per supplier, or summary reporting for internal stakeholder management.

Feature	Description
Sent questionnaires (these are the assessments you have sent to your supply chain as a MyCISO platform subscriber)	1. Setup questionnaire: a. Create a series of questions to dynamically determine supplier criticality b. Add custom questions per criticality level c. Select framework per criticality level 2. Send one questionnaire – Set Custom criticality level and confirm framework to be sent, or chose Dynamic Criticality for the supplier to respond to the dynamic criticality questions to determine their own criticality and receive the appropriate custom questions and framework. 3. Send multiple questionnaires – Download template csv, populate with your supplier details, then upload full supplier list to be sent out. 4. Reminder schedule – Set custom frequency reminder to all incomplete suppliers. The default frequency is every Monday at 9am. 5. Add a trusted supplier - A trusted supplier are those that have detailed public documentation available on their cyber maturity. E.g. Microsoft or AWS. 6. Our sent questionnaires: a. Lists all suppliers that you have sent an assessment to b. You can filter this list by i. View assigned to me ii. Trusted (i.e. trusted suppliers) iii. Certified (i.e. suppliers that have an approved certification) iv. Complete (i.e. suppliers that have been marked as completed) v. Notification (i.e. suppliers that have pending notifications for you to review) vi. Dynamic (i.e. suppliers who have been assigned a dynamic criticality) vii. Pending (i.e. suppliers who are have not yet completed the process) c. Supplier search 7. Supplier Detail (found by clicking on the supplier name): a. Summary of supplier details b. Supplier certified toggle

Feature	Description
	c. Supplier complete toggle d. Assign admin or staff member to supplier e. Vulnerability scan domain field f. Notifications centre g. Steps to finish tracker i. Company profile ii. Supplier questions iii. View assessment iv. Generate report – Once all steps are complete h. Documents (links) to files i. Calendar – Set reminders to partner j. Request supplier to complete assessment k. Notes free text field for internal notes not shared with the supplier l. Risks module to register and monitor supplier risks
Received questionnaires (these are the assessments you have received from another MyCISO platform subscriber)	1. Received questionnaires: a. Filter sent questionnaires based on filters b. Select from all received questionnaires to view progress 2. Active questionnaire: a. Summary of supplier details b. Notifications centre c. Steps to finish tracker d. Documents (links) to files 3. Generate report – Once questionnaire is complete
Response dashboard (Partner)	1. Supplier RAG status – Summary of Critical, Stable, Benchmark suppliers 2. Supplier criticality chart - % of Low, Medium, High criticality suppliers 3. Upcoming supplier calendar dates – Summary of all reminders across all suppliers 4. Latest notifications – Summary of latest updates across all active suppliers 5. Questionnaire responses table a. Filter by Criticality, Step completion, Notifications b. Summary of all active supplier questionnaires in sortable table 4. Export all data from questionnaire responses table 5. Export filtered data from questionnaire responses table
Vulnerability Detail	1. Sort the results on the page via domain name, scan level, or issue. 2. Review the vulnerability scan results per scanned domain.

Feature	Description
	a. Level 3 scans provide: i. Top level score out of 100 plus A - F grade ii. 10 Factor scores out of 100 iii. Full 200+ vulnerability scan with results broken down into severity b. Level 2 scans provide: i. Top level score out of 100 plus A - F grade ii. 10 Factor scores out of 100 c. Level 1 scans provide: i. Top level score out of 100 plus A - F grade
Vulnerability Licensing	1. Filter domains via scan level or status 2. Export your license summary 3. Add domains to be potentially licensed for scanning 4. Promote a validated domain to be scanned at level 1, 2, or 3 5. Base subscription includes a. 30 x level 1, 20 x level 2, and 1 x level 3 vulnerability scans
File Store	1. Repository for generated reports from both the Assess, Culture and Supplier modules. 2. Generate new report – Dynamic report generation based on frameworks completed and subscribed products. Schedule recurring reports.

8. MyCISO Metrics

The Metrics module is a comprehensive tool designed to empower security leaders with centralised control over the ongoing effectiveness of their security program. Included in the module are the abilities to:

- Set and track business wide metrics
- Reports for metrics and incidents

Feature	Description
Metrics configurations	1. Select from the MyCISO metrics that matter library consisting of more than 70 metrics 2. Set your gather frequency for the metrics 3. Configure each metric setting your business goal and the responsible staff member
Metrics	1. Use the metrics dashboard to track your progress against your selected metrics over time 2. Review each metric on each gather date against your set goal with a Red Amber Green status. 3. Select your metric gather date to adjust the any metric you are an admin on or assigned to. 4. Adjust the period you view your metrics over selecting from presets or custom dates. 5. Export your metric data to CSV. 6. Adjust the reminder settings for the staff members assigned to each metric. 7. View benchmark data for your selected metrics as compared to similar businesses. 8. Click on each metric to see the scores plotted over time or quickly adjust your goal

9. MyCISO Incidents

The Incidents module is a comprehensive tool designed to empower security leaders with the ability to build and run Incident Response Playbooks within the MyCISO app. Included in the module are the abilities to:

- Create incident playbook templates to assist in certification
- Manage and record cyber incidents as they occur

Incident configuration	1. View the preconfigured library of MyCISO incidents with over 15 templates. 2. Edit or duplicate a template to customise the incident type to your business. 3. Review attached risk ratings to each template based on incident to risk mappings.

	4. Add files to incident templates. 5. Set notifications for incident templates. 6. Configure playbooks attached to each incident template allowing you to move checkpoints from the library to quickly build a response plan. 7. Configure risks attached to incidents, you can adjust any of the risks in the MyCISO library to map to each template plus adjust the increased likelihood of the risk in the event of the incident occurring. 8. Set up contact lists attached to each incident template. 9. Configure checkpoints to be added to incident templates allowing you to quickly add notes and responsible parties to them. 10. Create a custom incident template. 11. Register a new incident against any template saved.
Incidents	1. Track incidents over time and how their occurrence affects overall business risk rating. 2. Register a new incident against a template. 3. Review days since incident, Days to contain incidents, Days to remediate incidents. 4. Filter incident log to find the Active, Resolved or False Positive types. 5. Sort incidents by Stage, Severity, Status, Registered by, Name. 6. Active incident control panel: a. Register dates and add notes and description to each stage of the active incident b. Add notifications and files to active incident c. Add classification and type to active incident d. Adjust risks, playbook and contact preferences e. Trigger notification to assigned staff against each checkpoint f. Send email update to contact list g. Set actual RTO and RPO h. Export incident log to csv i. Export incident timeline, 4 formats j. Close incident, reset risk levels or mark as false positive

10. SecurityOS Bundles

Our four SecurityOS bundles fit your journey, combining key features and reporting to cut effort and drive uplift.

10.1 Starter

For organisations starting their journey with MyCISO seeking a light-weight entry point, providing the Essentials Frameworks and the Precog AI automated framework, including 350 security controls answered automatically via API and external scans. Starter includes access the suite of MyCISO tools with entry level license coverage, to get you started.

10.2 Essentials

For organisations ready to take the next step in their security journey, Essentials expands upon the Starter tier with enhanced capability and depth. It more than doubles the number of controls within the Starter frameworks, providing broader coverage and stronger assurance.

Essentials introduces advanced reporting — including Essential 8 compliance insights — and extends visibility across your environment through vulnerability scanning and attack surface mapping. With integrated metrics management and actionable insights, Essentials builds a solid foundation for organisations to begin implementing a comprehensive security maturation programme.

10.3 Core

For organisations seeking the new gold standard in cybersecurity management, Core delivers the full power of the MyCISO Security Operating System. Building on the capabilities of Essentials, Core unlocks access to 65+ comprehensive frameworks — including NIST, Essential 8, GDPR, and more — enabling complete governance and compliance coverage.

Subscribers also gain full access to MyCISO's automated reporting modules, delivering rich insights and executive-grade dashboards. With the ability to manage up to five critical suppliers, Core provides the visibility, control, and automation needed to operate a mature, fully integrated security programme.

10.4 Enterprise

At the top of the MyCISO Security Operating System, Enterprise delivers a complete, integrated platform for large organisations managing complex cybersecurity, governance, risk, and compliance requirements.

Enterprise provides third-party risk management for up to 20 suppliers, along with advanced incident and risk management capabilities. It supports federated environments and discrete business units, enabling coordinated oversight across diverse organisational structures.

With supplier attack surface mapping, vulnerability scanning, and deep automation throughout, Enterprise helps teams consolidate and eliminate vendor and tool sprawl — ensuring comprehensive control, efficiency, and confidence across the entire security ecosystem.

10.5 Startup

Designed exclusively for emerging businesses, Startup delivers the full power of the MyCISO Enterprise tier — tailored specifically for organisations in their early growth phase.

It includes all the advanced capabilities of Enterprise, from comprehensive governance, risk, and compliance management to third-party oversight, vulnerability scanning, and attack surface mapping.

This special tier is available only to companies five years old or younger with fewer than 100 staff, and can be purchased once for a 1-, 3-, or 5-year term. Startup empowers growing organisations to establish enterprise-grade security foundations early — at a scale and structure that supports rapid, sustainable expansion.

11. SecurityOS Feature Comparison

Easily see which bundle delivers the right balance of features, reporting, and scalability for your needs.

Module / Feature	Starter	Essentials	Core	Enterprise
Assess				
Frameworks	ISO27001/NIST/ SOC-2 Starter, SMB1001 Bronze	ISO27001/NIST/ SOC-2 Essentials, Essential 8, SMB1001 all	All 65+ frameworks	All 65+ frameworks
PrecogAI automated assessment (350 controls)			✓	✓
Custom frameworks				
Maturity tracking over time	✓	✓	✓	✓
PrecogAI strategy	✓	✓	✓	✓
Benchmarking	✓	✓	✓	✓
Risk scenario assessment	✓	✓	✓	✓
Reports	Partial	✓	✓	✓
Comply				
Scope & SOA management			✓	✓
Audit management			✓	✓
Auditor view			✓	✓
Evidence management			✓	✓
Culture				
Strategy builder	✓	✓	✓	✓
CISO Masterclass series	✓	✓	✓	✓
Video learning catalogue		+	+	+
Reports & dashboards	✓	✓	✓	✓
Gamification			✓	✓
Phishing simulations		+	+	+

Module / Feature	Starter	Essentials	Core	Enterprise
Digital collateral			✓	✓
Printed Collateral		+	+	+
Suppliers				
Supplier assessment	5 sends	5 sends	5 sends	20 sends
Custom questions				
Frameworks				
Automated classification	✓	✓	✓	✓
Trusted suppliers		✓	✓	✓
Supplier improvement plan			✓	✓
External vulnerability scans		✓	✓	✓
Supplier risk register			✓	✓
Incidents				
30+ IR playbook templates		✓	✓	✓
IR playbook builder			✓	✓
IR SOP builder				
Incident manager				✓
Tabletop exercises			+	+
Vulnerabilities (CTEM)				
Continuous monitoring	✓	✓	✓	✓
Internal scan	✓	✓	✓	✓
Mapped to controls			+	✓
External scan		✓ Level 1	✓ Level 2	✓ Level 3
Connected Apps (API)		✓	✓	✓
Remediation Guidelines Level 4			+	+
Platform				
Reporting	✓	✓	✓	✓
Board reports	✓	✓	✓	✓
Control assessment	✓	✓	✓	✓
Risk scenario assessment	✓	✓	✓	✓
Improvement Strategy	✓	✓	✓	✓
ISO27001 report			✓	✓
NIST CSF 2.0 report			✓	✓
Essential 8 report		✓	✓	✓
Other framework specific reporting			✓	✓
Group account report			✓	✓
Toolbox				

Module / Feature	Starter	Essentials	Core	Enterprise
Templates & policies		Plus	✓	✓
Group Accounts				
Roll-up reporting			✓	✓
Subsidiary management			✓	✓
Group control management			✓	✓
Child accounts			+	+
Files & Evidence				
Central repository		✓	✓	✓
Version control		✓	✓	✓

Note: + indicates a paid add-on

12. MyCISO Add Ons

12.6 MyCISO Custom Framework

MyCISO can build a custom framework(s) from our Master Control Framework of over 1200+ controls to address your specific requirements for either an Assess or Suppliers framework.

12.7 Security Awareness Video - Advanced Edits

For changes to the animated series videos, voice-overs, graphics, custom SCORM, questions or content a SOW shall be created and agreed separately in writing with confirmation of effort/cost

12.8 Printed Collateral Pack

10 x 150gsm A2 posters, 1 pull up banner, 50 printed coasters, 50 pens, including delivery fee and brand customisation of posters.

12.9 MyCISO Security Elite Days

Security Elite is the custom vCISO service providing bespoke per day Professional Services for enterprises.

12.10 MyCISO Suppliers Bundle

The MyCISO Suppliers Bundle will add an additional 100 suppliers to the Suppliers Module. Must be purchased with Suppliers.

13. MyCISO Guided Setup

Each of the MyCISO modules can be bundled with guided setup if the customer is not on a Plus or Elite program. The guided setup for Assess, Suppliers, and Culture are typically run over 3 workshops where the customer is onboarded to the platform.

The activities included in guided setup for each of the modules is detailed below.

13.11 MyCISO Assess Guided Setup

Guided setup activities:

- Guided walk-through, onboarding, and setup of the Assess module
- Up to 3 maturity assessment discovery workshops (max 1 hour each) in the first month of subscribing to the MyCISO platform, aligned to your preferred framework
    - Including, 1 Risk Scenario assessment workshop
    - **Note**: Not all controls will be assessed during these workshops, some actions will be assigned to the customer between workshops
- MyCISO reports review, board report review and presentation session
- Walk through and training of the Assess platform and dashboard

13.12 MyCISO Culture Guided Setup

Guided setup activities:

- Guided walk-through, onboarding, and setup of the Security Culture module
- Up to 3 workshops (max 1 hour each) in the first month of subscribing to the MyCISO platform.
- Guidance on establishing a Cyber Resilience program, including:
    - Azure AD synchronisation
    - Stakeholder engagement
    - Change management: best practice on launching and operating a strategy
    - Remediation strategies
        - Overdue users
        - Repeat offenders in attack simulation
    - Identification and segmentation of your user groups, to create applicable tags in MyCISO
    - Guided creation of a multi-year Security Culture strategy, incorporating a range of learning activities for users
        - Who are your users? Learning needs, Types of activities

13.13 MyCISO Suppliers Guided Setup

Guided setup activities:

- Guided setup and walkthrough of the Suppliers module, detailing functionalities

- Up to 3 workshops (max 1 hour each) in the first month of subscribing to the MyCISO platform.
- Guidance on establishing a Third-Party Risk Management program, including:
    - Internal stakeholder engagement
    - Supplier/Vendor identification and inventory management
    - Framework selection and custom question development
    - Supplier onboarding
    - Sending initial assessments
    - Risk analysis, escalation, and reporting
    - Contract management
    - Due diligence and vendor selection process improvement
    - Continuous Monitoring and Regular Review
    - Stakeholder and board reporting

13.14 MyCISO Manage Guided Setup

Guided setup activities:

- Guided walk-through, onboarding, and setup of the **Manage** module
- Up to **3 onboarding workshops** (max 1 hour each) within the first month of subscribing to the MyCISO platform
- Introduction and configuration of the **Metrics Sub-Module**:
    - Selection of relevant cybersecurity metrics from the MyCISO Metrics Library
    - Assigning responsible owners and defining metric goals
    - Setting up data collection frequencies and reminders
- Introduction and configuration of the **Incidents Sub-Module**:
    - Review and customisation of incident response templates and playbooks
    - Defining incident types, severity levels, and escalation workflows
    - Assigning accountable contacts and setting notification preferences
- Walk-through of the **Manage dashboard** and training on:
    - Tracking metrics over time
    - Logging and managing incidents
    - Generating reports for stakeholders and boards
- Guidance on establishing a cadence for **ongoing cyber program review and reporting**

13.15 MyCISO Comply Guided Setup

Guided setup activities:

- Guided walk-through, onboarding, and setup of the **Comply** module (requires Assess)
- Up to **3 structured workshops** (max 1 hour each) in the first month of subscribing to the MyCISO platform

- Scoping the **Information Security Management System (ISMS)**:
    - Defining boundaries, stakeholders, key processes, and security objectives
    - Aligning ISMS scope with organizational context and ISO 27001 expectations
- Assistance with reviewing and structuring your **compliance documentation needs**
    - Policy and procedure gap identification
    - Mapping controls to ISO 27001 Annex A
- Walk-through and configuration of **compliance-related metrics** using the Manage module (if also enabled)
- Introduction to **board and audit-ready compliance reporting** within MyCISO
- Overview of the compliance **roadmap structure**, certification milestones, and role of internal audit

13.16 MyCISO SecurityOS Starter Guided Setup

The MyCISO SecurityOS Starter bundle provides access to core platform functionality through a self-guided onboarding process.

- No live onboarding sessions are included within this bundle.
- Subscribers to the Starter bundle are encouraged to access MyCISO University, which contains a comprehensive library of on-demand training videos, user guides, and knowledge articles.
- This resource supports customers in learning how to navigate and operate the platform, including step-by-step guidance on using the Assess, Culture, and Suppliers modules where available.
- All onboarding resources can be accessed at:
    - https://comms.myciso.co/s/article/MyCISO-University-Training-Content

Support is available through the in-platform Help Centre for technical queries or upgrade discussions.

13.17 MyCISO SecurityOS Essentials Guided Setup

The MyCISO SecurityOS Essentials bundle includes up to three (3) x 1-hour onboarding sessions, designed to introduce users to the core functionality available within their subscription.
The purpose of these sessions is to assist the customer in understanding how to effectively use each module to begin managing their cybersecurity program.

Session 1: Platform Setup and Assess Module Overview

- Overview of account setup, user management, and company profile configuration.
- Introduction to the **Assess module**, including framework selection and control maturity assessment.
- Guidance on:
    - how to commence a self-led assessment aligned to your chosen framework.
    - how to complete a risk assessment.

- how to generate reports once a gap and risk assessment are complete.

Session 2: Culture Overview

- Introduction to the **Culture module**, including awareness training workflows, phishing simulations, and engagement metrics.
- Guidance on:
  - AzureAD synchronisation
  - Identification and segmentation of your user groups, to create applicable tags in MyCISO
  - Guided creation of a multi-year Security Culture strategy, incorporating a range of learning activities for users
- Guidance on establishing your initial awareness campaigns and supplier assessments.

Session 3: Suppliers overview, Review and Next Steps

- Overview of the **Suppliers module**, including supplier classification, assessment setup, and review of supplier dashboards.
- Guidance on establishing a Third-Party Risk Management program, including:
  - Internal stakeholder engagement
  - Supplier/Vendor identification and inventory management
  - Framework selection and custom question development
  - Supplier onboarding
  - Sending initial assessments
- Review of early progress within modules and clarification of best-practice workflows.
- Guidance on generating reports and utilising insights for executive reporting.
- Discussion of options for extended support through **MyCISO Plus** or **MyCISO Elite** programs.

13.18 MyCISO SecurityOS Core Guided Setup

The MyCISO SecurityOS Core bundle includes **three (3) x 1-hour onboarding sessions** to familiarise users with the broader range of modules and reporting functionality included within their subscription.
These sessions provide structured guidance to enable customers to confidently self-manage their cybersecurity activities across multiple MyCISO modules.

Session 1: Platform Setup and Assess Module Overview

- Overview of account setup, user management, and company profile configuration.
- Introduction to the **Assess module**, including framework selection and control maturity assessment.
- Guidance on:
  - how to commence a self-led assessment aligned to your chosen framework.
  - how to complete a risk assessment.

- how to generate reports once a gap and risk assessment are complete..

Session 2: Culture and Suppliers Overview

- Introduction and overview of the **Culture module**, covering awareness strategy creation, training deployment, and metrics dashboards.
- Introduction and overview of the **Suppliers module** for managing third-party assessments, criticality levels, and supplier communications.

Session 3: Manage overview, Review and Next Steps

- Brief introduction to the **Manage module**, including incident and metrics sub-module awareness.
- Review of each module's initial setup and progress.
- Guidance on generating **board-ready reports** and monitoring cyber maturity metrics.
- Recommendations for maturing the program through the **MyCISO Plus** or **Elite** services.

13.19 MyCISO SecurityOS Enterprise Guided Setup

The MyCISO SecurityOS Enterprise bundle includes **three (3) x 1-hour onboarding sessions** to enable organisations to effectively deploy and oversee multiple MyCISO modules at scale. These sessions focus on enabling administrative confidence and providing foundational capability across all subscribed components.

Session 1: Enterprise Platform Orientation

- Overview of **account hierarchy**, **Group and Client accounts**, and role-based permissions.
- Introduction to the **Assess module** and guidance on coordinating multi-business unit assessments.
- Overview of control ownership and synchronisation for group-wide reporting.

Session 2: Supplier and Culture Enablement

- Guidance on configuring the **Suppliers module** for multi-tier supplier assessments and compliance tracking.
- Introduction to the **Culture module** to establish an enterprise-wide awareness program and monitor engagement metrics.
- Review of reporting workflows and visibility across subsidiaries or business units.

Session 3: Manage and Reporting Alignment

- Introduction to the **Manage module**, including use of **Metrics** and **Incidents** sub-modules.
- Guidance on scheduling and generating consolidated reports across modules.
- Discussion on integrating additional governance layers through **MyCISO Elite** for ongoing program maturity and executive enablement.

13.20 MyCISO SecurityOS Startup Guided Setup

The MyCISO SecurityOS Startup bundle includes **three (3) x 1-hour onboarding sessions** tailored to assist smaller organisations or new cybersecurity programs in effectively using the platform to build foundational maturity.

Session 1: Getting Started

- Overview of platform fundamentals, user roles, and key settings.
- Introduction to the **Assess module** for initial framework selection, control maturity assessment, and reporting.
- Guidance on using built-in recommendations to prioritise first improvement actions.

Session 2: Building a Security Culture and Managing Suppliers

- Introduction to the **Culture module** for awareness training and phishing simulation setup.
- Overview of the **Suppliers module** to begin evaluating third-party risks.
- Guidance on interpreting early results to drive improvement.

Session 3: Review and Maturity Planning

- Review of activities completed in the first two sessions.
- Assistance with generating early reports and communicating outcomes internally.
- Overview of optional maturity uplift programs available through **MyCISO Plus** and **Elite**.

14. MyCISO Plus

MyCISO Plus provides a light-touch vCISO engagement throughout the course of the annual subscription, where MyCISO will provide guidance to the customer during a 1-hour call, once a month, on how to progress their cyber improvement journey.

The Plus program is aligned with each MyCISO module. If support is required across multiple modules, then multiple Plus programs need to be established to support the appropriate area.

14.21 MyCISO Assess Plus

MyCISO Assess Plus is a guided, advisor-led program designed to help customers implement the Assess module effectively and build momentum toward security maturity uplift. The program includes onboarding support, recurring reviews, and targeted advisory to optimise the value of the platform and support strategic security planning.

Support is provided by the **MyCISO Delivery Team**, with contributions from a **Security Consultant** or **Account Manager** depending on the subject matter.

Assess Plus Support Activities:

- **Onboarding and Platform Enablement**
  - Guided walk-through and configuration of the Assess module
  - Up to **3 onboarding workshops** (max 1 hour each) in Month 1
    - Includes a **Risk Scenario Assessment** workshop
    - Framework-aligned maturity discovery and control review
  - Platform navigation training, report generation, and roadmap walkthrough
- **Monthly Strategic Advisory Calls**
  Up to 12 x 1-hour calls available throughout the year. Topics may include:
  - Crown Jewels and Business Impact Analysis
  - ISMS Scoping and documentation support
  - Security Roadmap Planning and prioritisation
  - Framework Alignment and gap interpretation (e.g., NIST, ISO 27001, CPS 234)
  - Policy Development and review
  - Risk Management Strategy setup
  - Incident Response Planning
  - Awareness and Culture Integration
  - Third-Party Risk Management
  - Audit Preparation and Control Attestation
- **Additional Benefits**
  - Includes **3 x Level 2 Vulnerability Scans**
  - Ad-hoc platform usage support via help@myciso.co, subject to reasonable use

14.22 MyCISO Culture Plus

MyCISO Culture Plus provides proactive, light-touch guidance for organisations implementing the MyCISO Culture module. The engagement begins with onboarding workshops and continues with optional monthly check-ins to support execution, troubleshoot challenges, and mature your awareness strategy over time.

Support is delivered by the MyCISO Delivery Team, with involvement from a MyCISO Security Consultant or your Account Manager as needed.

Culture Plus Support Activities:

- **Onboarding and Platform Setup:**
  - Guided walk-through and configuration of the Security Culture module
  - Azure AD synchronisation support
  - Creation and mapping of user tags and groups
- **Awareness Strategy Enablement:**
  - Identification and segmentation of users
  - Creation of a multi-year strategy via the Strategy Builder
  - Scheduling of eLearning, attack simulations, and engagement assets
- **Resilience Uplift Guidance:**
  - Remediation support for:
    - Overdue users
    - Repeat offenders in phishing simulations
  - Behavioural insight review from dashboards
- **Stakeholder Coaching:**
  - Guidance on stakeholder engagement and change management
  - Option to support internal launch communications and awareness campaigns
- **Ongoing Monthly Reviews:**
  - Monthly check-in calls to review strategy execution and performance
  - Optional use of the meeting for a **Strategic Security Review**, covering:
    - Threat landscape update
    - Program observations
    - Platform roadmap
    - Investment summary
- **Ad-hoc advisory** support available via help@myciso.co, subject to reasonable use.

14.23 MyCISO Suppliers Plus

MyCISO Suppliers Plus delivers proactive, advisor-led support for implementing and maturing your third-party risk management (TPRM) program using the MyCISO platform. Designed for organisations that want to establish a sustainable and scalable supplier security process, this service combines hands-on setup, structured advisory, and recurring engagement over 12 months.

The engagement is led by the MyCISO Delivery Team, with input from a Security Consultant or Account Manager, and is structured to deliver both foundational success and ongoing program momentum.

Key Contacts for Calls:

- MyCISO Delivery Team
- MyCISO Account Manager

Customer Success Core Support Activities:

- **Onboarding & Platform Setup**
  - Guided setup of the MyCISO Suppliers module
  - Dashboard training, reporting walkthroughs, and scan enablement
  - Initial onboarding workshops covering:
    - Stakeholder engagement and RACI modelling
    - Supplier inventory and criticality classification
    - Assessment methodology design (including inherent risk criteria)
    - Procurement and project “gate” integration points
    - Internal communication and platform training for key teams
- **Supplier Onboarding & Assessment Launch**
  - Assistance preparing supplier engagement comms
  - Advisory on custom frameworks and question sets by supplier type
  - Guidance on assessment rollout and risk attribute tagging
  - Support interpreting early responses and scan results
- **Structured Escalation & Exception Management**
  - Advisory on how to handle **non-conforming suppliers**
  - Escalation comms templates and engagement workflows
  - Tracking unresolved issues and prioritising next steps
- **Executive Reporting & Board Advisory**
  - Support preparing stakeholder and board-level reporting
  - Guidance on **quarterly metrics**, trends, and supplier segmentation
  - Visualisation of supplier maturity and risk exposure using platform dashboards
- **Continuous Improvement Touchpoints**
  - Quarterly review of scan usage, reassessment targets, and supplier exceptions
  - Program health check: supplier status changes, high-risk trends, and platform use optimisation

Included Usage

- 100 supplier assessments
- Vulnerability scans:

- 30 x Level 1
- 40 x Level 2
- 3 x Level 3

- Ad-hoc advisory via help@myciso.co, subject to reasonable use

14.24 MyCISO Manage Plus

MyCISO Manage Plus is designed to provide proactive support to customers leveraging the Manage module for cybersecurity oversight, metrics tracking, and incident response. The engagement includes a series of initial onboarding activities and workshops, followed by an option for regular monthly calls to review and enhance your security program execution using the Manage capabilities.

The support is delivered by a combination of the MyCISO Delivery Team, a MyCISO Security Consultant, or your Account Manager depending on the activity and needs.

Key Contacts for Calls:

- MyCISO Delivery Team
- MyCISO Account Manager

MyCISO Manage Plus Support Activities:

- Guided walkthrough and onboarding of the Manage module, including:
  - Configuration of key metrics aligned to organisational goals
  - Setup and customisation of incident response templates and playbooks
- Guidance on operationalising security management, including:
  - Best practice for cyber KPI selection and stakeholder reporting
  - Mapping cyber metrics to risk themes and compliance requirements
  - Aligning incident playbooks with organisational risk scenarios and escalation paths
- Incident Response Support:
  - Assistance in establishing incident classification and prioritisation
  - Setup of communication workflows, stakeholder contact lists, and RTO/RPO tracking
  - Creating a repeatable incident response and remediation rhythm
- Monthly Security Program Review:
  - Use your monthly call to review incidents, metrics trends, or risk deviations
  - Option to conduct a Strategic Security Review Meeting, leveraging a defined template to cover:
    - Threat landscape updates
    - Key incident learnings
    - Investment alignment
    - Platform configuration recommendations
    - Program roadmap and reporting progress
- Board and Executive Reporting:
  - Support in using dashboard data to create outcome-focused reports suitable for board consumption or audit committee briefings
- Ad-hoc advisory requests may be submitted to help@myciso.co, subject to reasonable use.

14.25 MyCISO Manage Plus – Suggested 12-Month Timeline

Focus: Operational setup, platform utilisation, light-touch strategy support

Timeline	Focus Area	Outcome
Weeks 1–3	Onboarding & Guided Setup	Familiarisation with the modules, onboarding of stakeholders
Month 1	Metrics Program Setup	Core KPIs defined, assigned, and tracked; dashboard live
Month 2	Incident Playbook Configuration	Key IR templates reviewed, customised, and published
Month 3	Assigning Owners & Automation Setup	Stakeholders assigned; reminders and reporting cadences configured
Month 4	Initial Incident Log Review & Testing	IR flow tested with a sample incident; RTO/RPO added
Month 5	Establish Reporting Cadence	Metrics/incident summary report templates prepared; review cadence agreed
Month 6	Risk-Informed Metrics Review	Adjusted KPIs to match risk register alignment (if Assess module used)
Month 7	Stakeholder Engagement Checkpoint	Mid-year executive checkpoint; updates based on user feedback
Month 8	Trends & Insights Review	Quarterly report package created; deltas and remediation themes identified
Month 9	Dashboard Optimisation & Filtering	Dashboards refined for board/audit needs
Month 10	Continuous Improvement & Scenario Planning	Introduce simple tabletop/simulation walkthrough
Month 11	Annual Metrics & Incident Summary Drafting	Prepare annual review report (cyber scorecard)
Month 12	Final Strategic Review & Planning	Recap year's outcomes; define roadmap for next year

14.26 MyCISO Comply Plus

The MyCISO Comply Plus Service offers proactive support for customers focusing on ISO 27001 implementation and compliance. The engagement includes initial onboarding activities, workshops, and an optional monthly call for strategic guidance, ensuring organizations can align with ISO 27001 standards efficiently and effectively.

Key Contacts for Calls:

- MyCISO Delivery Team
- MyCISO Account Manager

Customer Success Core Support Activities:

Plus Program Scope:

- Guided setup and walkthrough of the Suppliers module, detailing functionalities
- Guided ISO 27001 Implementation:
    - Assistance in scoping the Information Security Management System (ISMS) specific to ISO 27001.
    - Facilitate initial assessments, gap analysis, and control maturity evaluation exclusively within the ISO 27001 framework.
- Monthly Strategic Guidance:
    - Monthly 1-hour guidance sessions to review progress on ISO 27001 implementation, focusing on policy development, control implementation, and audit readiness.
- Metrics-Driven Compliance Tracking:
    - Leverage the Metrics module in Manage to track progress against key milestones in the compliance journey, ensuring transparency and accountability.
- Board and Stakeholder Reporting:
    - Support in developing ISO 27001-aligned compliance reports that are board-ready and address both operational and strategic objectives.
- Third-Party Risk Management:
    - Assistance in integrating third-party assessments to ensure alignment with ISO 27001 requirements for supplier risk management, including frameworks for evaluating supplier compliance.
- Cyber Awareness as a Compliance Point:
    - Ensure alignment between the organization's ISO 27001 compliance and its Cyber Awareness efforts. Provide guidance on implementing awareness programs as part of compliance objectives.
- Limited Internal Audit Support:
    - Guidance on self-assessments or limited internal reviews of ISO 27001 compliance progress.

15. MyCISO Assess Elite

MyCISO Assess Elite is a structured, outcome-led engagement that delivers an end-to-end maturity uplift across your cybersecurity program. Designed for organisations seeking full strategic alignment, the program covers gap assessments, stakeholder reporting, roadmap planning, and implementation support — all tailored to your organisational goals and risk context.

The program is executed at a pace that suits your commercial readiness, typically over a 6–12 month horizon.

- **Includes 3 x Level 3 vulnerability scans**

Activity	Objective	Key Deliverables
1. Onboarding & Platform Enablement	Establish a baseline of maturity and enable the Assess module for structured delivery.	- Full setup and configuration of the Assess module - Framework selection and alignment - Control maturity assessment workshops - Risk scenario assessment and prioritisation - Generation of board-ready baseline and improvement strategy reports
2. Crown Jewels & Business Impact Analysis	Identify and prioritise the protection of critical assets and business functions.	- Facilitation of crown jewels discovery workshop - Confidentiality, integrity, and availability (CIA) classification - Mapping assets to business functions - Documentation of ownership, dependencies, and supporting controls
3. Risk Management Framework	Establish a practical and business-aligned framework to identify and manage cyber risks.	- Development of a tailored risk methodology - Integration of risk heatmaps from MyCISO - Risk treatment planning and ownership assignment - Setup of ongoing monitoring and review process
4. ISMS Scoping	Define the structure, stakeholders, and boundaries of the Information Security Management System.	- Clear ISMS scoping aligned to ISO 27001 or relevant framework - Stakeholder engagement mapping - Inclusion/exclusion boundary definition - Integration points with other business units and governance functions
5. Security Roadmap & Budget Planning	Translate strategic priorities into a phased roadmap and align with resourcing and budget.	- Definition of control uplift phases based on risk and effort - Strategic roadmap with 3–12 month horizons - Budget recommendations and planning support - ROI alignment and executive-ready business cases

6. Security Policy Review & Development	Review, draft, or enhance policies to ensure alignment with frameworks and business realities.	- Gap analysis of current policies - Policy drafting or updates aligned to ISO, NIST, or internal standards - Stakeholder workshops to validate policies - Governance and approval guidance
7. Incident Response Planning	Build or enhance the organisation's ability to respond to and recover from security incidents.	- Development of an IR plan aligned to risk scenarios - Role definition and escalation workflow - Facilitation of tabletop or simulation exercise - Integration with BCP/DR and continuous review loops
8. Framework Alignment & Compliance Planning	Ensure consistent alignment to selected frameworks and support audit readiness.	- Control mapping and gap resolution across selected framework(s) - Advisory on selecting the right framework for business context - Alignment to compliance goals (e.g., ISO 27001, CPS 234) - Executive reporting templates for audit trail and evidence gathering
9. Board & Stakeholder Reporting	Equip leadership with confidence and clarity on cyber posture and program progress.	- Creation of tailored reporting packs (KPIs, risks, progress) - Support for quarterly reporting cycles and board briefings - Visualisation of maturity uplift and residual risk - Feedback loop facilitation to adjust strategy based on exec inputs
10. Awareness & Culture Integration	Embed behavioural change into your broader maturity uplift efforts.	- Identification of awareness gaps and risk-based learning needs - Strategic alignment with Culture module (if used) - Training prioritisation based on maturity gaps - Executive guidance on fostering long-term cyber behaviour change
11. Third-Party Risk Management Enablement	Connect Assess outcomes to your supply chain security strategy.	- Identification of critical third-party risks linked to internal controls - Guidance on integrating Assess with Suppliers module (if used) - Support on vendor security requirements and contract alignment
12. Audit & Attestation Preparation	Prepare for external reviews and demonstrate control effectiveness and maturity.	- Support for pre-audit readiness checks - Evidence collation and control owner preparation - Mapping outputs to attestation/reporting templates - Guidance on auditor Q&A and walkthroughs

15.27 Optional Extras – MyCISO Assess Elite

Optional Activity	Objective	Key Deliverables
1. Control Ownership & Delegation	Establish operational accountability across business units for control implementation.	- Control owner assignment mapping - RACI model development - Cross-functional governance register - Guidance on embedding ownership into BAU
2. Internal Security Comms Planning	Drive internal buy-in beyond the executive layer.	- Cyber uplift communication templates - "You own this control" briefing sheets - Messaging playbook for HR/IT/comms - Internal champion identification
3. Integration with Existing Tools	Connect Assess outputs into existing GRC, project, or reporting platforms.	- CSV/API export guidance - Integration mapping (ServiceNow, Jira, etc.) - Optional dashboards (e.g., Power BI, Google Studio) - Template for aligning actions with PMO tickets
4. Capability Maturity Benchmarking	Help stakeholders understand and contextualise maturity ratings.	- Business-aligned maturity target setting - Peer-level or industry qualitative benchmarking - Dashboard visual aids for explaining levels - Mapping of levels to operating expectations
5. Change Management Enablement	Improve roadmap adoption through stakeholder engagement and structured change.	- Stakeholder mapping template - "Security Uplift Change Plan" template - Briefings on ADKAR or Kotter-style change methods - Risk mitigation playbook for security resistance
6. Cyber Risk Quantification (Lite)	Translate technical risk into business language and financial exposure.	- Risk quantification methodology (lite version) - Sample calculations using FAIR-lite or CVA-lite - Impact heatmaps translated to dollar terms - Executive summary framing for financial audiences
7. Assess Light for Business Units	Enable smaller teams or subsidiaries to perform streamlined assessments.	- Pre-configured "lite" assessment pathway - Top 5 risk scenarios only - Simplified roadmap and controls - Training on decentralised roll-out model

16. MyCISO Culture Elite

The MyCISO Culture Elite Program delivers a fully managed, strategic approach to cybersecurity awareness and behaviour change. This program is ideal for organisations seeking to go beyond check-the-box training and build a truly embedded security culture.

The program is executed over a 12-month period and combines guided implementation, behavioural reinforcement, peer advocacy, and measurement to elevate workforce cyber resilience.

Activity	Objective	Key Deliverables
1. Onboarding & Guided Setup	Introduce the program and establish baselines	- Kick-off briefing and onboarding - Conduct baseline phishing simulation - Distribute initial awareness materials
2. Platform Enablement	Tailor platform to organisation's needs	- Azure AD sync setup - User tags and segmentation - Strategy configuration (cadence, learning paths) - Simulation environment configured
3. Training Program Launch	Deploy training and assess engagement	- Launch of eLearning and assets - Track early engagement and feedback - Adjust delivery as needed
4. Simulation & Testing	Reinforce training through attack simulations	- Phishing simulation rollout - Post-campaign review and debrief - Dashboard insights shared with stakeholders
5. Policy Framework Review	Align awareness to organisational policies	- Review current awareness policy - Recommend and draft updates (if needed)
6. Communication Strategy	Promote cyber awareness across the org	- Develop awareness messaging plans - Schedule newsletters, briefings, and event collateral
7. Cyber Ambassador Program	Empower champions and peer learning	- Identify and train ambassadors - Define roles/responsibilities - Coordinate monthly ambassador sessions
8. Remediation & Support	Address knowledge gaps and reinforce learning	- Create remediation workflows for low performers - Align offline engagement strategies with training cadence
9. Sustainability Planning	Embed culture long term	- Develop ongoing learning roadmap - Integrate awareness into onboarding and BAU - End-of-year impact assessment and improvement plan

17. MyCISO Suppliers Elite

The Suppliers Elite Program provides end-to-end support in managing third-party cybersecurity risk, engaging stakeholders and establishing governance to ensure alignment across your organisation. We assist in building a comprehensive supplier inventory and developing or refining a methodology for supplier assessments.

Our team facilitates staff training and communication, guides supplier onboarding, and manages assessment questionnaires and vulnerability scans. Each response is reviewed to build fourth-party awareness, with risk assessments and critical vulnerability triage conducted to prioritise issues. Non-conforming third parties are documented, escalated, and re-evaluated as needed, while continuous monitoring ensures sustained compliance and risk mitigation.

- 100 supplier assessments are included, as standard.
- Provides vulnerability scanning of third parties and reporting, including
    - 95 x Level 2 vulnerability scans
    - 5 x level 3 vulnerability scans

Activity	Overall Objectives	Key Activities
1. Governance & Stakeholder Alignment	Establish ownership and alignment for third-party risk governance across the organisation.	- Guided setup in the Suppliers module - Create or uplift policies related in collaboration with key stakeholders - Establish criteria for evaluating third party security risks - Establish procedures to measure third party inherent risks and assess risk performance - Build reporting metrics and cadence for periodic reporting to internal stakeholders (monthly or quarterly) - Ensure that people, process and technology are optimised for the organisation's risk objectives
2. Supplier Inventory & Categorisation	Create a complete and structured supplier list to support criticality-based risk management.	- Build an inventory of all third party suppliers across the business from the procurement database - Implement processes to identify new third parties and changes to existing third parties - Categorise suppliers into 'High, 'Medium' and 'Low' criticality - Identifying third parties and changes to existing parties enables the organisation to engage in risk processes
3. Assessment Methodology & Risk Criteria	Develop a standardised and scalable supplier assessment process.	- Review or implement procurement process gates to be included in contracting new third parties and changes to existing supplier relationships - Implement IT gates in projects that require new third parties or changes to existing third parties - Build a RACI matrix and define roles and responsibilities to ensure effective collaboration, accountability and communication throughout the supplier assessment process

4. Internal Training & Communication	Enable internal teams and supplier managers to execute their roles in TPRM.	- Promote the third-party risk program to inform stakeholders of relevant policies, standards and operating procedures - Train third-party personnel with sensitive access to the organisation's assets - Train users who will be interacting with the platform on how to use the Supplier Module
5. Supplier Engagement & Assessment Launch	Ensure suppliers understand the process and complete their assessments efficiently.	- Contact suppliers and inform them about the assessment process - Conduct initial risk assessments and assign each party a risk rating based on their supply chain risk exposure - Capture inherent risk attributes such as services, data types, connectivity
6. Vulnerability Scanning & Triage	Detect and prioritise supplier exposure using external scan data.	- Add primary and secondary domains to a supplier assessment - Uplift licenses as appropriate for the level of scanning required - Review potential risks as discovered via the vulnerabilities feature - Suppliers Elite subscription includes a. 70 x level 1 vulnerability scans b. 25 x Level 2 vulnerability scans c. 5 x level 3 vulnerability scans
7. Response Analysis & Fourth-Party Awareness	Review assessments and surface risks across your extended ecosystem.	- Present a dashboard on the current risk supply chain posture - Determine assessment frequency based on residual risk rating for continuous assessment - Assess responses from third parties according to established standards and methodology - Build an understanding of service providers used by the third parties
8. Risk Escalation & Issue Management	Actively manage non-conforming suppliers through structured escalation.	- Build understanding of vendors' critical vulnerabilities and their mitigation action plans
9. Documenting and Escalating Non-Conforming Third Parties	Ensure repeatable, well-governed action is taken when suppliers don't meet expectations.	- Discuss the status of issues with third parties - Adjust the assessment plan based on prior assessments or continuous surface assessment results - Assist in the curation of communications to the non-conforming suppliers and build a strategy for the organisation to address the issues, which may include: a. Follow-up Communications: Send follow-up communications, both via email and the platform by setting clear deadlines for response in these communications.

		b. Escalation: If there is still no response after follow-ups, escalate the issue through the monthly review meetings with the organisation. c. Assessment of Impact: Assess the criticality of the supplier to the organisation operations. If they are categorised as high criticality, their non-compliance poses a greater risk, and more effort should be made to engage them. d. Risk Management Plan: Develop a risk management plan for the possibility that the supplier remains non-compliant. e. Contractual Measures: The organisation should maintain contractual agreements with the supplier and ensure there are clauses that require them to comply with such assessments. f. Final Ultimatum: If all attempts fail, issue a final ultimatum stating the consequences of non-compliance, which could range from ceasing business with them to legal actions, depending on the severity of the risk they pose and the legal framework of the agreements between the organisation and the supplier. g. Documentation: Document all communications and steps taken for internal audit purposes, demonstrating due diligence in managing supplier risks, and may be necessary if legal actions are taken.
11. Program Reporting & Stakeholder Engagement	Communicate program progress and risk status to leadership and internal owners.	- Share assessment results with the third parties and the internal stakeholders - Record assessments in a risk register and take mitigation actions - Compliance tracking: Monitor suppliers' adherence to the agreed cybersecurity standards and policies during previous activities. - Risk identification and escalation: Respond to risks or incidents within the supply chain as they are discovered. - Incident management and response: Escalate urgent issues discovered through the continuous scanning mechanisms to the organisation point of contact. - Performance review meetings: Facilitate monthly/quarterly meetings to report the progress of the programme of work, highlighting exceptions and discoveries.
11. Program Reporting & Stakeholder Engagement	Communicate program progress and risk status to leadership and internal owners.	- Risk register updates with supplier input - Documentation of assessment changes and risk actions - Compliance tracking support - Stakeholder sharing workflows
12. Continuous Monitoring & Improvement	Ensure long-term program success and adaptability in a dynamic threat environment.	- Reporting and dashboard updates: MyCISO platform provides a real-time dashboard as well as comprehensive reports detailing the risk posture, compliance status and trends - Supplier engagement and feedback: Maintain regular communication with suppliers to gather feedback and

		provide updates in order to maintain transparency, trust and accountability throughout the supplier lifecycle. - Continuous improvement: Use insights gained from the programme to refine and enhance third-party risk assessment process and methodologies for future engagements - Review the supplier assessment process to identify areas for improvement that could increase engagement rates in the future.

17.28 Ongoing Value Streams Available in the Supplier Elite Program

Area	Why It Matters	How We Stay Involved
Risk-Based Reassessment Planning	Supplier environments change. Customers need help knowing when and who to reassess.	- Help build reassessment cadence (e.g., high-risk: 6 months, medium: annually)
		- Quarterly check-in on overdue or upcoming assessments
Supplier Exception Monitoring & Escalation Guidance	Non-conformance doesn't stop at the initial review. They need help actioning it.	- Review flagged suppliers
		- Coach through response plans
		- Escalation comms templates
Quarterly Program Reporting Support	Most orgs struggle to summarise activity and outcomes for leadership.	- Help them prep executive reports using dashboard data
		- Include: completion stats, high-risk suppliers, fourth-party insights, trends
Supplier Comms Strategy Support	Keeping suppliers engaged and compliant requires ongoing effort.	- Provide templates or touchpoints for reminder comms
		- Quarterly newsletter or "status reminder" copy support
New Supplier Onboarding Support	Customers will add new vendors throughout the year.	- Help assess risk rating of new suppliers
		- Advisory on which assessment to send
		- Assistance setting them up in the platform
Scan License Strategy & Refresh	Vulnerability scan use needs to be planned and targeted.	- Quarterly review of usage
		- Recommend reallocations/upgrades
		- Triage of scan results
Risk Posture Trending	Leadership wants to see improvement or at least visibility.	- Compare current vs. previous quarter's supplier maturity data
		- Highlight top improvers and deteriorators
		- Recommend remediation focus areas
Platform Usage Coaching	New team members, feature updates, or changes in use cases.	- Light training refreshers
		- Review and optimise workflows
		- Tag management / report building tips

Regulatory or Audit Support (if applicable)	May be requested to show evidence of supplier due diligence.	- Help extract and format data
		- Provide narrative for audits or internal reviews

17.29 Example Recurring Activities Timeline (Months 3–12)

Month	Advisory Touchpoint Focus
3	Review early supplier completions
	Recalibrate supplier comms (who's unresponsive?)
4	Build executive summary report for leadership
	Revisit high-risk responses
5	Scan utilisation check-in
	Support any new supplier onboarding
6	Reassessment cadence review (start planning Q2-Q3 vendors)
	Help tag exceptions
7	Supplier reminders support
	Performance trends: who's improving/deteriorating?
8	Executive reporting refresh
	Prep quarterly board slide (if applicable)
9	Posture trending report
	Fourth-party discoveries update
10	Support new supplier classification
	Refresh question sets if needed
11	Pre-audit summary or health check
	Scan license usage wrap-up
12	End-of-year performance review
	Recommendations for next 12 months

18. MyCISO Manage Elite

The MyCISO Manage Elite Program delivers a structured, outcome-driven approach to elevating your cybersecurity oversight capability. Designed for organizations seeking proactive cyber risk governance, the program leverages the full power of the *Manage* module to build maturity across cyber metrics, incident response, executive reporting, and continuous improvement.

This program supports cybersecurity and risk leaders in establishing consistent visibility, accountability, and stakeholder engagement across their security program — all aligned to business objectives, compliance requirements, and real-world threats.

18.30 Program Highlights

- **Foundational Setup and Governance Design**
  - Facilitation of kick-off workshops to align cyber oversight goals with organizational strategy and risk posture.
  - Definition of a governance model for cyber metrics, reporting lines, and incident ownership.
  - Integration of the Manage module into existing operating rhythms (e.g., risk and compliance committees, audit & exec reviews).
- **Metrics Program Enablement**
  - Design of a custom cyber metrics framework aligned with regulatory, risk, and performance management needs.
  - Selection of meaningful KPIs and KRIs from the MyCISO Metrics Library, mapped to controls and business impact.
  - Implementation of data collection and reporting cadence, with responsible owners, targets, and escalation triggers.
  - Continuous oversight to optimize performance indicators, drive engagement, and surface gaps.
- **Incident Response Maturity Building**
  - Build or enhance incident response playbooks tailored to your top risks (e.g., ransomware, third-party breach, business email compromise).
  - Support development of escalation paths, response timelines, and post-incident workflows.
  - Design of incident classification schema and alignment to organizational risk appetite.
  - Coordination of simulation and tabletop exercises to validate readiness and promote cross-functional collaboration.
- **Executive and Board Reporting Uplift**
  - Advisory on building outcome-focused cyber dashboards and executive-level views.
  - Development of reporting templates aligned to board, regulator, or audit expectations.
  - Contextualization of cyber data to tell a story: risk drivers, business impact, trend analysis, and confidence in program performance.
- **Risk-Driven Program Oversight**

- Regular cadence of program reviews and recalibration, driven by performance, new threats, and strategic shifts.
- Continuous improvement loops across incidents, metrics, and management actions.
- Integration of real-world risk scenarios into incident planning and reporting alignment.

- **Cross-Program Synergies and Integration**
  - Aligning Manage module practices with outputs from other modules (e.g., Assess risk data, Culture engagement insights, Supplier findings).
  - Creation of joined-up reporting across strategy, performance, and third-party assurance.
  - Support for mapping outcomes to compliance frameworks (e.g., ISO 27001, CPS 234, SOCI), without becoming a formal certification program.

18.31 Program Flexibility

The **Manage Elite Program** is structured to operate over a 12-month period, with workstreams aligned to your organization's pace, resource availability, and maturity uplift objectives. Engagements are sequenced to prioritize foundational capability first (metrics and playbooks), followed by continuous improvement, executive engagement, and scenario-driven evolution.

This model ensures you build a **repeatable, measurable, and board-ready cyber governance program** that evolves alongside your business — without introducing unnecessary complexity.

18.32 MyCISO Manage Elite Deliverables:

- **Strategy & Governance Workshops**
  - Cybersecurity management maturity review
  - Stakeholder mapping and governance alignment
  - Facilitation of security objectives setting and board engagement model
  - Definition of operating cadence for cyber program reviews, risk meetings, and reporting
- **Metrics Program Design**
  - Design and configuration of a **custom metrics framework** tailored to business objectives and compliance mandates (e.g., ISO 27001, CPS 234, SOCI)
  - Prioritisation of "metrics that matter" for board and operational reporting
  - Definition of KPIs and KRIs aligned to cyber, business continuity, and operational risk
  - Assignment of responsible parties and automated reminders via the platform
  - Support for benchmarking against industry peers (where available)
- **Incident Response Enablement**
  - Design and build of **customised incident playbooks** based on threat scenarios (e.g., ransomware, BEC, insider threat, supplier breach)
  - Mapping of **RTO/RPO targets**, escalation pathways, and response roles
  - Facilitation of **simulation exercises** to test readiness and response time
  - Post-incident lessons learned process and continuous improvement loops
- **Risk and Compliance Integration**
  - Alignment of Manage workflows to your existing GRC or compliance framework

- Development of risk classification schema and control dependencies
- Identification of high-impact events and residual risk tracking via incident data

- **Board and Regulator Reporting**
  - Creation of **executive-ready reporting templates**, integrating:
    - Program maturity updates
    - Control effectiveness trends
    - Metrics performance summaries
    - Incident volumes, root causes, and response metrics
  - Advisory on reporting cadence and storytelling for non-technical audiences
- **Quarterly Strategic Reviews**
  - Executive review of progress across metrics, incidents, and roadmap actions
  - Re-calibration of focus areas based on performance and stakeholder feedback
  - Program roadmap refinement based on organisational change or threat evolution
- **Additional Support**
  - **Ad-hoc advisory requests** available via help@myciso.co, subject to fair use
  - Optional coordination with **internal audit, legal, or risk functions** to align oversight model

18.33 MyCISO Manage Elite – Suggested 12-Month Timeline

Focus: Strategic governance uplift, cross-functional coordination, executive-level program oversight

Timeline	Focus Area	Outcome
Weeks 1–3	**Onboarding & Governance Workshops**	Cyber oversight model defined; executive sponsor engaged; platform configured
Month 1	**Custom Metrics Framework Design**	Strategic KPIs/KRIs aligned to risk appetite and compliance requirements
Month 2	**Incident Response Operating Model**	Playbooks finalised; escalation paths and roles documented
Month 3	**Data Collection & Stakeholder Reporting Setup**	Owners assigned; reminders and templates in place
Month 4	**Executive & Board Reporting Templates**	Tailored visualisations, dashboards, and language to match audience expectations
Month 5	**Incident Simulation & Lessons Learned Workflow**	Conduct IR exercise; initiate post-incident review loop
Month 6	**Cross-Program Integration (Assess / Culture / Suppliers)**	Metrics and incidents linked to strategy, awareness gaps, or third-party risks

Month 7	**Maturity Model & Benchmarks Review**	Program maturity visualised; compared with peers or baseline
Month 8	**Scenario-Based Risk Planning (e.g., Ransomware, Insider Threat)**	IR plan expanded to include scenario-specific response logic
Month 9	**Compliance Reporting Alignment (ISO 27001, CPS 234, SOCI)**	Metrics mapped to audit controls; evidence-ready dashboards created
Month 10	**Quarterly Executive Debrief & Planning**	Strategic checkpoint; priorities recalibrated
Month 11	**End-of-Year Performance Summary**	Detailed report on incidents, trends, metrics, program evolution
Month 12	**Roadmap Creation for Next Year**	Strategic focus areas agreed for following 12 months

19. MyCISO Comply Elite

The **MyCISO Comply Elite Program** provides a comprehensive and tailored approach to achieving ISO 27001 compliance and enhancing your organization's overall security maturity. Designed for organizations requiring hands-on, end-to-end guidance, the program ensures a seamless journey through compliance assessment, implementation, and certification readiness.

19.34 Program Highlights

- **Groundwork Establishment and Strategic Planning**
  - Scoping the Information Security Management System (ISMS) to align with ISO 27001 requirements, focusing on your organization's unique context and objectives.
  - Conducting a detailed gap analysis to identify areas requiring attention.
  - Strategic communication planning to ensure alignment with executive leadership and stakeholders.
- **Comprehensive Implementation Support**
  - Development and refinement of policies, procedures, and control documentation to meet ISO 27001 standards.
  - Assistance in the selection and implementation of security controls, leveraging industry best practices.
  - Creation of a risk management framework tailored to ISO 27001 requirements, ensuring effective risk identification, treatment, and monitoring.
- **Stakeholder Reporting and Roadmap Development**
  - Board-ready reporting to ensure transparency and accountability throughout the compliance journey.
  - Detailed roadmap planning with phased milestones for achieving certification.
  - Budget planning to align compliance efforts with organizational resources and priorities.
- **Incident Response and Business Continuity Planning**
  - Development or enhancement of an incident response plan and business continuity strategy in line with ISO 27001 Annex A controls.
  - Facilitation of testing and refinement exercises to ensure readiness and resilience.
- **Training and Awareness Integration**
  - Integration of cyber awareness programs to support compliance efforts and foster a culture of security.
  - Role-specific training to ensure all team members understand their responsibilities under the ISMS.
- **Audit Preparation and Certification Support**
  - Pre-audit reviews and guidance to address potential non-conformities.
  - Mock audit exercises to ensure readiness for external certification assessments.

- Assistance in managing third-party audits to ensure smooth progression to certification.

19.35 Program Flexibility

The Comply Elite Program is tailored to your organization's pace, with activities structured to align with your commercial viability and change management capacity. The timeline is adjustable, ranging from as short as 6 months to as long as 24 months, based on your organization's goals and readiness for implementation.

With the **Comply Elite Program**, your organization benefits from a hands-on, strategic partnership, ensuring you achieve ISO 27001 certification while building a robust and sustainable compliance framework.

19.36 Elite Program Scope

- **Dedicated vCISO Oversight**:
  - Provide a **vCISO** to oversee ISO 27001 compliance efforts, including the management of internal audit functions as the organization produces required policies and processes.
  - Ensure internal audits meet ISO 27001 requirements and address areas for improvement.
- **Advanced Metrics-Driven Compliance Monitoring**:
  - Full integration with the **Metrics module in Manage** to track compliance journey milestones. Include deeper insights and trend analyses for continuous improvement.
- **ISO 27001 Policy and Process Development Support**:
  - Provide expertise in drafting and refining policies and procedures required for ISO 27001 compliance, ensuring alignment with audit expectations and operational goals.
- **Comprehensive Cyber Awareness Programs**:
  - Develop and deliver cyber awareness training aligned with ISO 27001's compliance requirements. Focus on building employee resilience against human error as a key part of the organization's compliance efforts.
- **Third-Party Risk Management**:
  - Full-service support for supplier compliance, including assessing third-party risk, ensuring ISO 27001 alignment, and creating tailored risk management strategies.
- **Internal Audit Function**:
  - Provide structured internal audits as part of the compliance process, ensuring policies, procedures, and controls align with ISO 27001 requirements.
- **Ongoing Compliance and Improvement Workshops**:
  - Facilitate workshops for ISO 27001 topics, such as internal audits, risk management, and policy alignment. Include detailed guidance for transitioning from gap analysis to readiness for certification.
- **Advanced Reporting and Metrics**:

- Generate detailed compliance progress reports, including tailored recommendations for executives and board presentations. Provide trend data to show improvement over time.

20. Product Naming Convention

Change Date	Type	Old Name	New Name
23rd April 2025	Added Manage and Comply modules, including Plus and Elite program descriptions	NA	NA
1st May 2024	Product rename	Assess Customer Success Security Culture Customer Success Suppliers Customer Success	Assess Plus Culture Plus Suppliers Plus
1st November 2023	New product	Managed Security Program	MyCISO Security Elite
1st November 2023	New product	Customer Success	Assess Customer Success Security Culture Customer Success Suppliers Customer Success
1st November 2023	New product	NA (Launch)	Group Account
1st November 2023	Product SKU ended	Security Culture – Engage	N/A
1st November 2023	Product SKU ended	NA (Launch)	Security Culture – Attack Simulation
1st November 2023	Product SKU ended	NA (Launch)	Security Culture – E-Learning
1st November 2023	Product SKU ended	NA (Launch)	Security Culture – Attack Simulation
1st July 2022	New product	NA (Launch)	Managed Security Program
1st July 2022	New product	NA (Launch)	Guided Setup
1st July 2022	New product	NA (Launch)	Customer Success
1st July 2022	New product	NA (Launch)	Security Consulting

1st July 2022	New product	NA (Launch)	Security Culture – Engage
1st July 2022	New product	NA (Launch)	Security Culture – Attack Simulation
1st July 2022	New product	NA (Launch)	Security Culture – E-Learning
1st July 2022	New product	NA (Launch)	Security Culture – Attack Simulation
1st July 2022	New product	NA (Launch)	Customer Success
1st July 2022	New product	NA (Launch)	Security Culture Complete
1st July 2022	New product	NA (Launch)	Assess
4th April 2023	New product	NA (Launch)	Suppliers