

Product Overview

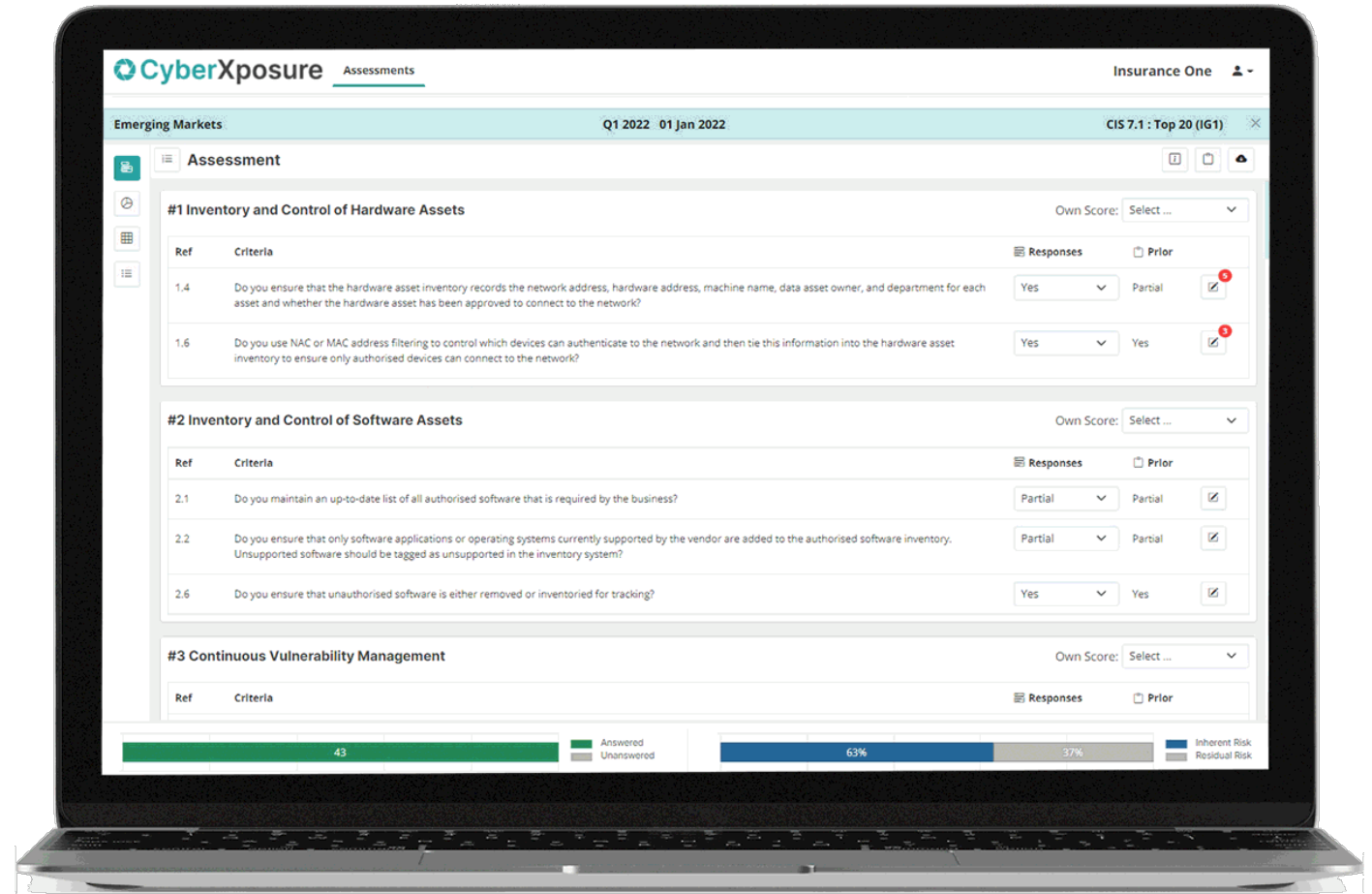


Totally understand your Cyber Security Status

Visualize your Cyber Security status throughout your entire organization across divisions, departments, locations.

- Review your position with a new assessment monthly, quarterly, bi-annually or annually.

Choose the security framework you wish to follow, CIS 8.0 | NIST



360° view of your organization's Cyber Security position

All information in one place, see all history and trends.



Quick setup

Get going quickly, choose your templates CIS or NIST, set up your business units, start managing your Cyber Security in a structured manner.



Easy to use

Once you are set up, you can easily create and manage your periodic Cyber Security reviews and obtain meaningful risk action plans, trend analysis and consolidated views of your Cyber Security position.



Customizable

Choose the security protocol that suits your organization and use recommended subsets of controls for your size of company.



Reduce Risk

Very quickly identify areas of concern from the Risk Action Plan. Remedy risks for a specific assessment by providing a remediation quotation linked to the assessment.



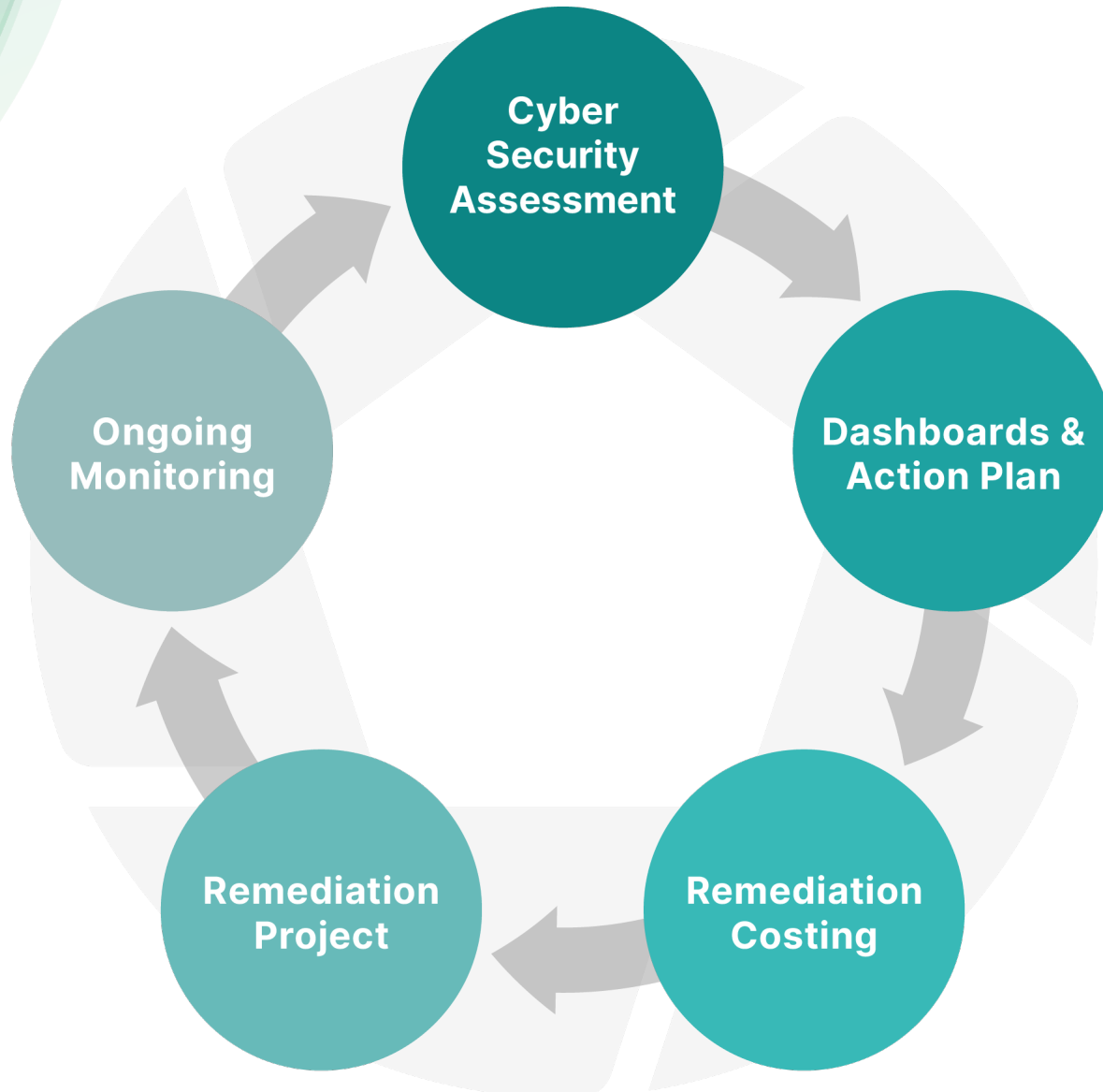
Work collaboratively

Work together or remotely, collaborate with your team across geographic regions. Work with your team to create a remediation budget. Manage the remediation project by exporting the remediation budget tasks to project management software.



CISO board view

The CISO board view can demonstrate your cyber security status and show all efforts at compliance with clear graphical representations of current and prior status. Demonstrate live Cyber Security status to your board, drill down into details where required.



The CyberXposure Cycle

Cyber Security Assessments



Assessments

- Set up how often you wish to do reviews - monthly, quarterly, bi-annually or annually.
- Define your team with relevant permissions for access.
- Using our assessment templates, simply determine the templates and sub-sets of templates you want to use (CIS 8.0 IG1,2,3 / NIST CSF 1.1 Profile1,2,3,4).
- Then set up your units - these could be subsidiary companies, departments, locations, separate businesses for consultants. Any way you wish to divide organizations.
- Once these actions are completed you can start your 1st assessments.

CyberXposure Assessments Templates Units Settings Users Insurance One

Assessment Listing

New Assessment

Emerging Markets			
01 Jan 2022 Q1 2022 CIS 7.1 : Top 20 (IG1)	InProgress	43 Answered Unanswered	63% 37% Inherent Risk Residual Risk
01 Oct 2021 Q4 2021 CIS 7.1 : Top 20 (IG1)	Complete	43 Answered Unanswered	62% 38% Inherent Risk Residual Risk
01 Jul 2021 Q3 2021 CIS 7.1 : Top 20 (IG1)	Complete	43 Answered Unanswered	48% 52% Inherent Risk Residual Risk
Head Office			
01 Jan 2022 Q1 2022 CIS 7.1 : Top 20 (IG1)	InProgress	43 Answered Unanswered	100% Inherent Risk Residual Risk
01 Sep 2021 Q3 2021 CIS 7.1 : Top 20 (IG1)	Complete	43 Answered Unanswered	51% 49% Inherent Risk Residual Risk
01 Jul 2021 Q3 2021 CIS 7.1 : Top 20 (IG1)	Complete	43 Answered Unanswered	44% 56% Inherent Risk Residual Risk
Investment Group			
01 Jan 2022 Q1 2022 CIS 7.1 : Top 20 (IG1)	InProgress	43 Answered Unanswered	100% Inherent Risk Residual Risk
01 Sep 2021 Q3 2021 CIS 7.1 : Top 20 (IG1)	Complete	43 Answered Unanswered	48% 52% Inherent Risk Residual Risk
01 Jul 2021 Q3 2021 CIS 7.1 : Top 20 (IG1)	Complete	43 Answered Unanswered	45% 55% Inherent Risk Residual Risk

Assessment Capture

- Review each framework control and criteria.
- Set your expected score for the control then score each criteria.
- Add notes and files, “Evidence of Activity”.
- View results in graphs and the Risk Action Plan at any point.
- Motivate the Board for budget to remediate.
- Take action based on recommendations in the Risk Action Plan.

The screenshot displays the CyberXposure Assessment interface for 'Emerging Markets' on '01 Jan 2022'. The interface is organized into five main assessment sections, each with a table of criteria and a corresponding 'Evidence of Activity' panel on the right.

Assessment Summary: Q1 2022 01 Jan 2022 | CIS 7.1 : Top 20 (IG1)

Assessment #1: Inventory and Control of Hardware Assets (Own Score: 0)

Ref	Criteria	Responses	Prior
1.4	Do you ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network?	Yes	Partial
1.6	Do you use NAC or MAC address filtering to control which devices can authenticate to the network and then tie this information into the hardware asset inventory to ensure only authorised devices can connect to the network?	Yes	Yes

Assessment #2: Inventory and Control of Software Assets (Own Score: 0)

Ref	Criteria	Responses	Prior
2.1	Do you maintain an up-to-date list of all authorised software that is required by the business?	Partial	Partial
2.2	Do you ensure that only software applications or operating systems currently supported by the vendor are added to the authorised software inventory. Unsupported software should be tagged as unsupported in the inventory system?	Partial	Partial
2.6	Do you ensure that unauthorised software is either removed or inventoried for tracking?	Yes	Yes

Assessment #3: Continuous Vulnerability Management (Own Score: 0)

Ref	Criteria	Responses	Prior
3.4	Do you deploy automated software update tools to ensure that the operating systems are running the most recent security updates?	Partial	Partial
3.5	Do you deploy automated software update tools to ensure third-party software on all systems are up to date?	Partial	Partial

Assessment #4: Controlled Use of Administrative Privileges (Own Score: 0)

Ref	Criteria	Responses	Prior
4.2	Before deploying any new asset, do you change all default passwords according to a defined standard?	Partial	Partial
4.3	Do you ensure that all users with administrative account access use a dedicated or secondary account for elevated activities? This account should only be used for administrative activities and not internet browsing, email, or similar activities.	Yes	Yes

Assessment #5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers (Own Score: 0)

Ref	Criteria	Responses	Prior
5.1	Do you maintain documented security configuration standards, where applicable, for all operating systems and software?	Partial	Partial

Evidence of Activity Panel:

- Assessment: Q4 2021 01 Oct 2021
Date: 02 Mar 2022 10:38
By: October notes & image
[31848.jpg](#)
- Assessment: Q4 2021 01 Oct 2021
Date: 02 Mar 2022 10:38
By: October notes
- Assessment: Q3 2021 01 Jul 2021
Date: 02 Mar 2022 10:38
By: Testing Jun 2021 notes & image
[landy1.jpg](#)
- Assessment: Q3 2021 01 Jul 2021
Date: 02 Mar 2022 10:37
By: Testing Jun 2021 notes & document
[PERMACULTURE.docx](#)
- Assessment: Q3 2021 01 Jul 2021
Date: 02 Mar 2022 10:37
By: Testing Jun 2021 just some notes

Summary: 43 Unanswered | 63% Answered | 37% Inherent Risk Residual Risk

Dashboards and action plan

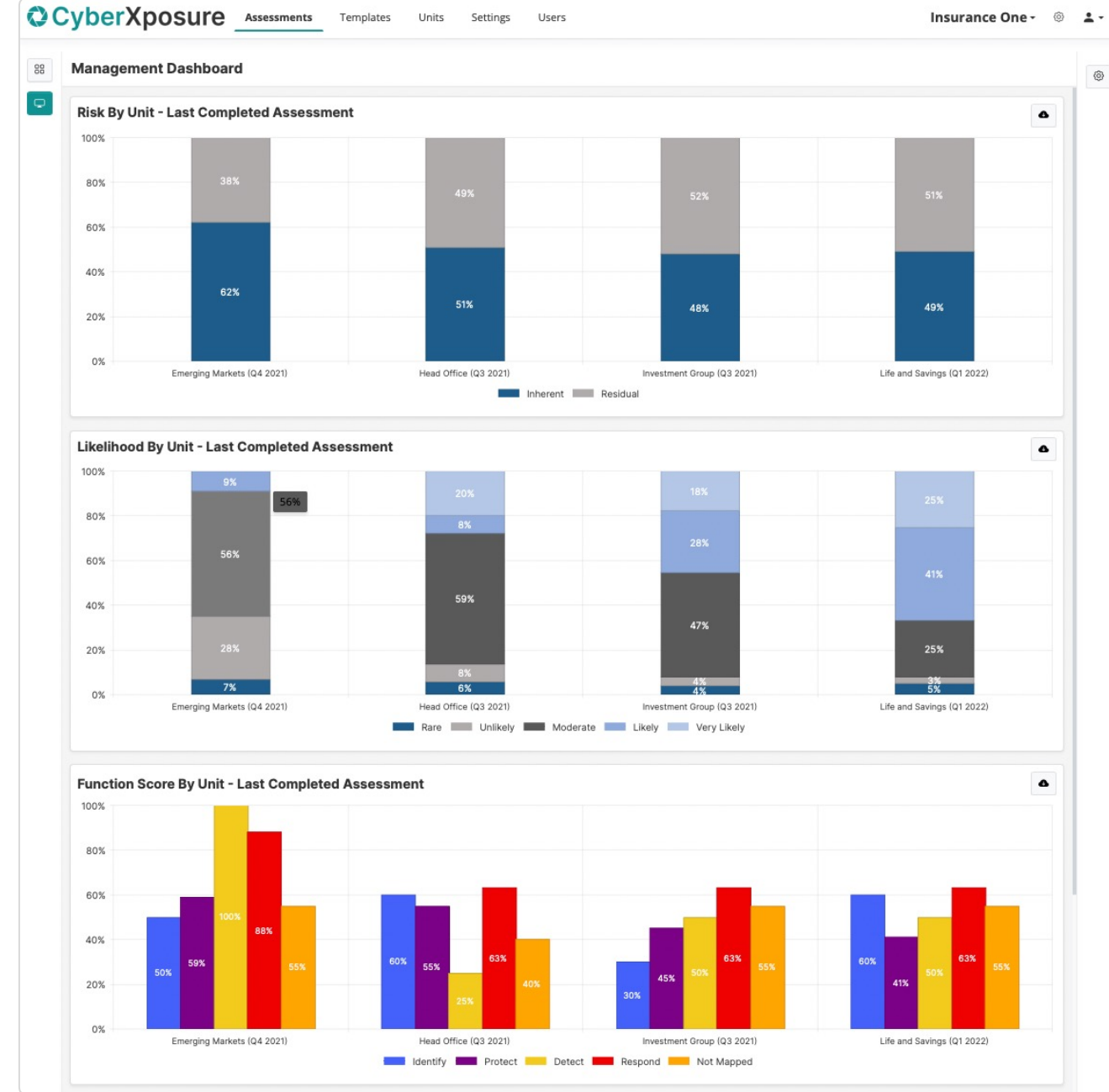


Management Dashboard

- The ability to look at your cyber-resilience status as an entire organisation is critical for management. Depending on how you have split your organisation - subsidiaries, departments, locations, equipment types, at some point you want to look at the entire organisation and compare across these.

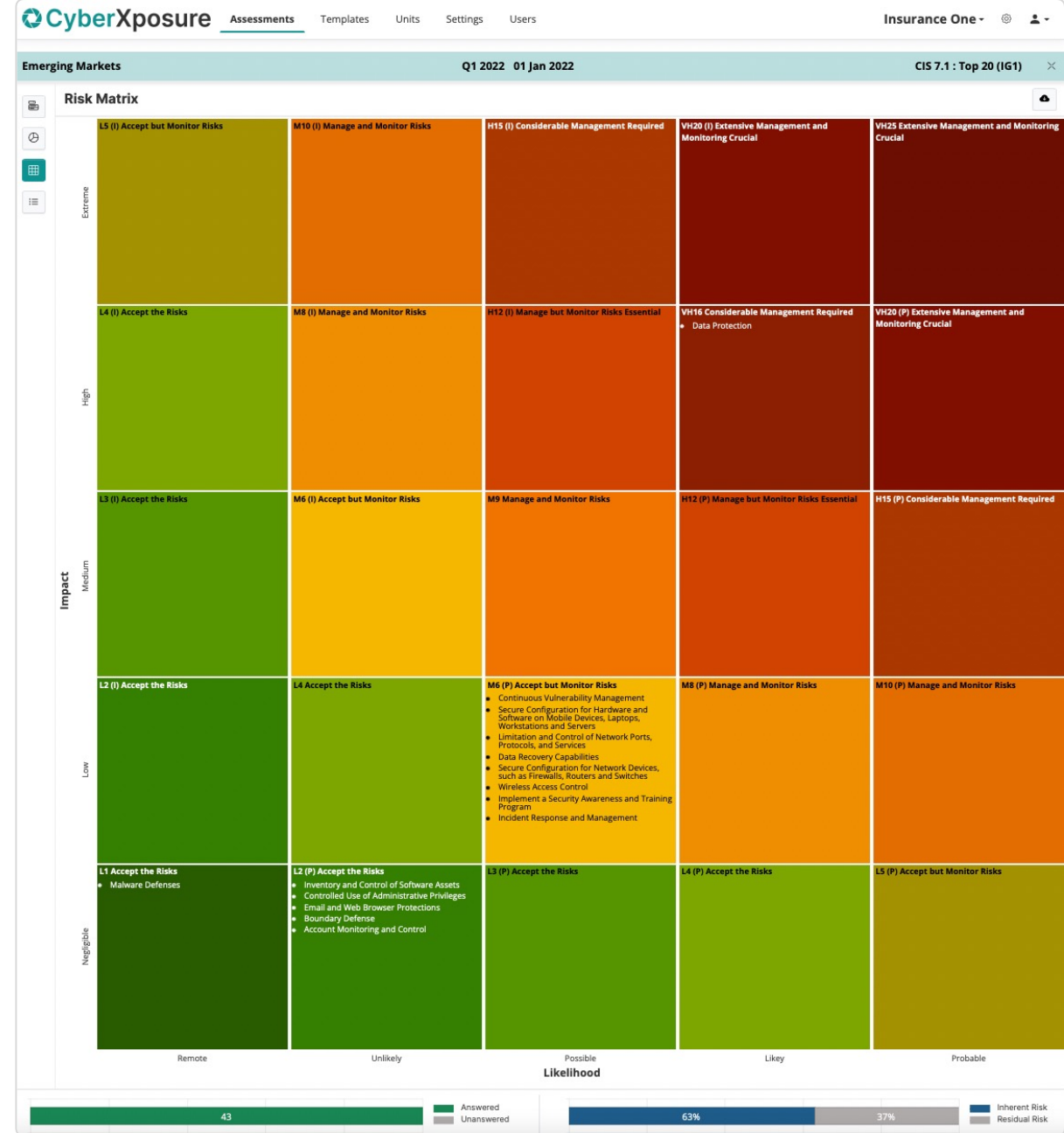
Our management dashboard graphically provides:

- Inherent vs Residual Risk by Unit.
- Event likelihood by Unit.
- NIST Function score by Unit (Both for NIST and CIS based frameworks).
- Residual Risk by Unit across time.
- These are key to being able to report on progress (or lack thereof) to the organisation's leaders as required.



Risk Matrix

- Our risk matrix looks at two axes, Impact and Likelihood. The grid of 25 blocks enables a very quick view of the controls / functions and where they fall in the matrix based on likelihood and impact.
- This analysis shows in one glance the areas of concern, colour coded to warn of danger.
- All reports, graphs and images can be exported for inclusion in external reports.



Assessment Dashboard

- View an assessment for business unit compared to previous assessments.
- Look at Risk distribution, Likelihood Distribution, Function Scores (CIS and NIST), Control Ratings and comparisons, detailed assessment results.
- Add notes and files as “Evidence of activity”, build a full repository of Cyber Security information for each business unit.



Risk Action Plan

- When an assessment is in progress, we dynamically create a Risk Action Plan. This tells you exactly what actions need to be performed, all graded by KPI's, in order to move from a non-conforming to conforming position.
- When an assessment is completed, it may be that not all risk areas have been resolved. These remain available to view as a risk register and are actionable at any point, when the next review period comes up the issues can be set as completed.
- The Risk Action Plan is a key differentiator of our service, enabling the easy identification, risk and action definition and forms the basis for our remediation budget/quotation.

CyberXposure Assessments Templates Units Settings Users Insurance One - CIS 7.1 : Top 20 (IG1)

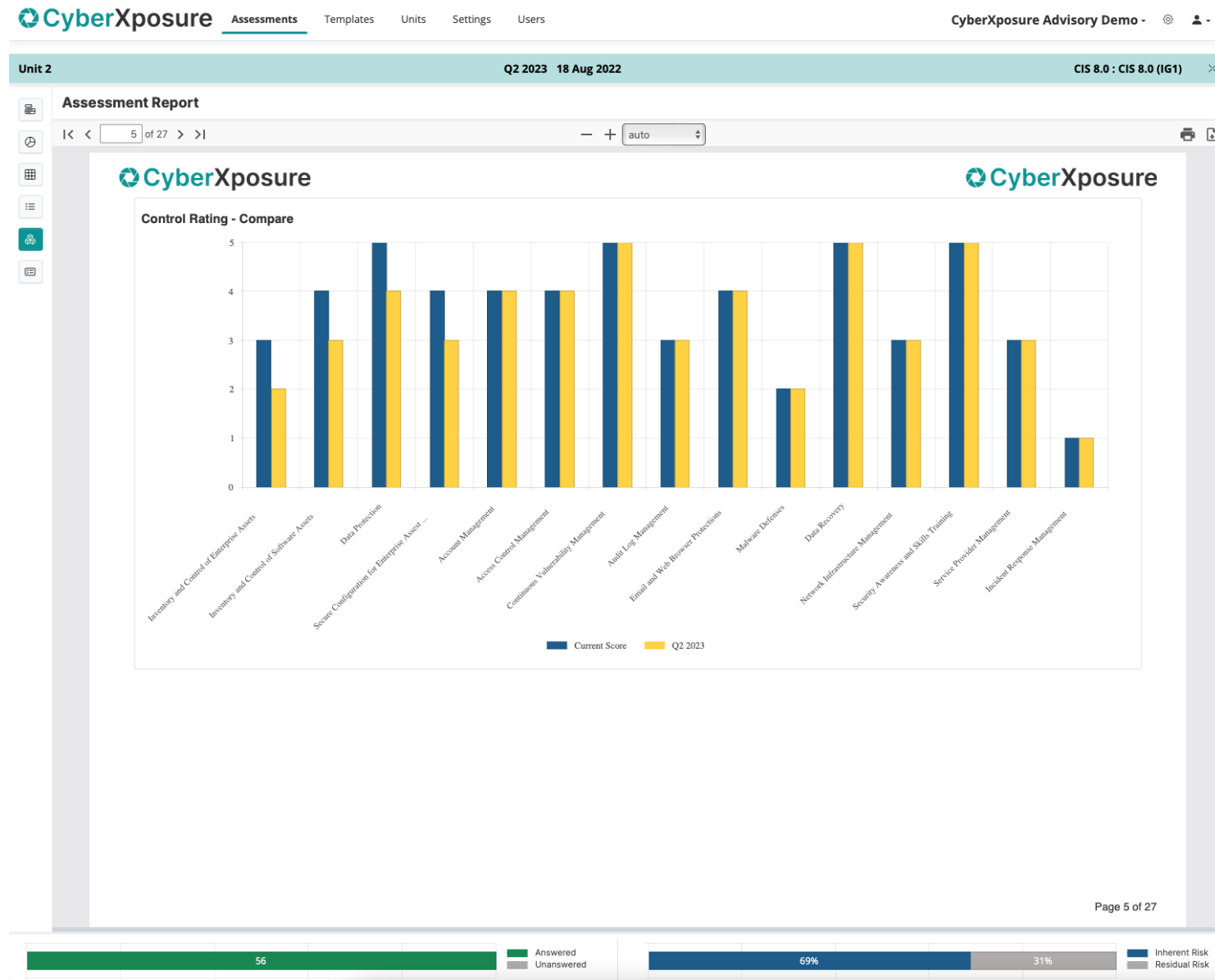
Emerging Markets Q1 2022 01 Jan 2022

Risk Action Plan

Control	Matrix	Priority	Likelihood	Effort	Impact	Exposure
#1 Inventory and Control of Hardware Assets		5	Rare	Low	Insignificant	
Control	Matrix	Priority	Likelihood	Effort	Impact	Exposure
#2 Inventory and Control of Software Assets	L2 (P)	4	Unlikely	Medium	Insignificant	Minor
Risk	Impact	Action				
2.1 Do you maintain an up-to-date list of all authorised software that is required by the business?						Partial <input checked="" type="checkbox"/>
Unsupported and out-of-date software can introduce risk.	Unsupported and out-of-date software create an opportunity can cause system interruptions, failures and introduce possible weaknesses.	Review the software asset list.				
2.2 Do you ensure that only software applications or operating systems currently supported by the vendor are added to the authorised software inventory. Unsupported software should be tagged as unsupported in the inventory system?						Partial <input checked="" type="checkbox"/>
Outdated and unsupported software can cause system interruptions.	An outdated software inventory can easily lead to critical systems being overlooked when vendors announce EOL or EOS for certain software versions. This will introduce the risk of systems being disrupted and can be seen as an internal threat.	Review the authorised software inventory and make sure unsupported software is tagged for removal.				
Control	Matrix	Priority	Likelihood	Effort	Impact	Exposure
#3 Continuous Vulnerability Management	M6 (P)	3	Moderate	Medium	Minor	Moderate
Risk	Impact	Action				
3.4 Do you deploy automated software update tools to ensure that the operating systems are running the most recent security updates?						Partial <input checked="" type="checkbox"/>
Outdated Operating Systems are often a target for attack.	Out of date security updates make operating system vulnerable for attacks. Hackers often focus their efforts on security flaws.	Review the automated software update tools for all platforms.				
3.5 Do you deploy automated software update tools to ensure third-party software on all systems are up to date?						Partial <input checked="" type="checkbox"/>
Unpatched or outdate versions of 3rd party software introduce a large attack surface on systems.	3rd party application patching is often overlooked, especially on critical systems due to the possible impact patching might have on the system or application. This is a known practice and thus an area targeted by threat actors.	Review the automated software update tools for 3rd party applications.				
Control	Matrix	Priority	Likelihood	Effort	Impact	Exposure
#4 Controlled Use of Administrative Privileges	L2 (P)	4	Unlikely	Low	Insignificant	Minor
Risk	Impact	Action				
4.2 Before deploying any new asset, do you change all default passwords according to a defined standard?						Partial <input checked="" type="checkbox"/>
Defined standard to chane default passwords on newly deployed assets is not adequate.	Either no defined standard is implemented to change default passwords on new asset that are deployments, or the standard is not being enforced.	Review defined standard for ensuring default passwords are changed.				

Export Risk Action Plan

- At any point export a full assessment report in pdf format.
- Use this report for internal liaison and discussion.
- Use the report to send to CISO, or to present to board.
- Communicate current cyber health status and proceed to remediation budget/quotation building.



Remediation costing



Remediation Costing

- This is a critical task, how to budget / quote your client on their remediation. The best way is based on the assessment. We offer a full budget/quotation methodology based on risk and impact.
- Build a full remediation cost model with services and products to enable a prioritised and executable plan for remediation.
- We cater for services:
 - Once off or recurring.
 - Assurance / Consulting / Managed Services .
- We cater for products:
 - Our service identifies product types required based on the assessment.
 - Our service may recommend products to remedy issues.
 - Products can be Once off or recurring.
 - SAAS and Standard.
- Improve your process to all stakeholders with the deliverables of a Risk Action Plan as well as a Fully detailed Remediation Budget to ensure full Cyber Resilience.

The screenshot displays the CyberXposure Remediation Budget interface. The top navigation bar includes 'Assessments', 'Templates', 'Units', 'Settings', and 'Users'. The user is logged in as 'HMS Family Trust'. The current assessment is 'IG 1 Assessment' for 'Q3 2023 01 Sep 2022'. The interface is divided into three main sections: '#1 Inventory and Control of Enterprise Assets', '#2 Inventory and Control of Software Assets', and '#3 Data Protection'. Each section contains a table of criteria with columns for 'Criteria', 'Answer', 'Action', and 'Control Framework'. Below each criteria table, there are tables for 'Once-off' and 'Recurring' remediation items, including columns for 'Item Type', 'Description', 'Period', 'UOM', 'Qty', 'Rate', 'Amount', and 'Annualised'. A 'Summary' panel on the right provides a breakdown of costs for 'Services' and 'Products', including 'Grand Total' and 'Please note: All recurring services and products have been annualised'. At the bottom, a progress bar shows 45% completion, with 11 items answered and 62% of the budget allocated.

Criteria	Answer	Action	Control Framework
1.1 Do you establish and maintain a detailed enterprise asset inventory?	No	Create an inventory that contains all the technology assets with the potential to store or process information, whether these technology assets are connected to the network or not.	Control Framework + Add Remediation
1.2 Do you address unauthorized assets every week?	Partial	Ensure that the implemented controls and processes that are used to respond to unauthorized assets are enforced weekly for all the unauthorized assets.	Control Framework + Add Remediation

Item Type	Description	Period	UOM	Qty	Rate	Amount	Annualised
Consulting	Determine Asset Inventory Requirement	Once-off	Hours	16	175	\$ 2,800.00	\$ 2,800.00
Assurance	Manage Unauthorised Assets	Week	Hours	1.5	100	\$ 150.00	\$ 7,800.00

Criteria	Answer	Action	Control Framework
2.1 Do you establish and maintain a software asset inventory of all the licenced software that is installed on the enterprise's assets?	Partial	Ensure that the business authorized software asset list is up to date with all the licensed software that is installed on the enterprise's assets.	Control Framework + Add Remediation
2.2 Do you ensure that only authorized software, that is currently supported by the vendor, is listed in the software asset inventory, for all the enterprise assets?	Yes	Regularly review the enterprise's software asset inventory to make sure it is up to date with the latest vendor-supported software that has been approved for organization use. Unsupported vendor software that has been approved for business use must be identified and documented in the IT risk register.	Control Framework + Add Remediation

Criteria	Answer	Action	Control Framework
3.1 Do you establish and maintain a data management process?	Partial	Ensure that a data management process is implemented for all the systems in the environment that process data.	Control Framework + Add Remediation
3.2 Do you establish and maintain a data inventory, based on the enterprise's	Partial	Ensure that all the sensitive and critical data to the enterprise is inventoried regardless of whether that data is located on-site or	Control Framework + Add Remediation

Category	Amount
Services	\$ 10,600.00
Once-off Consulting	\$ 2,800.00
Recurring Assurance	\$ 7,800.00
Products	\$ 4,200.00
Once-off	\$ 2,000.00
Recurring	\$ 2,200.00
Grand Total	\$ 14,800.00
Once-off	\$ 4,800.00
Recurring	\$ 10,000.00

Remediation Costing communication

- Export the full remediation costing to pdf.
- Meet stakeholders and present the budget.
- Prioritize and phase the remediation project, amend the costing and prepare to export the project tasks to Excel.

CyberXposure Assessments Templates Units Settings Users CyberXposure Advisory Demo - CIS 8.0 : CIS 8.0 (IG1)

Unit 2 Q2 2023 18 Aug 2022

Remediation Budget

1 < 3 of 5 > | auto

Services

#1 Inventory and Control of Enterprise Assets M6 (P)

Criteria	Answer	Action	Control Framework
1,1 Do you establish and maintain a detailed enterprise asset inventory?	No	Create an inventory that contains all the technology assets with the potential to store or process information, whether these technology assets are connected to the network or not.	Asset inventory management process, Enterprise asset inventory

Item Type	Description	Period	UOM	Qty	Rate	Amount	Annualised
Once-off							
Consulting	Plan and research asset inventory software	Once-off	Hours	4	100	\$ 400.00	\$ 400.00

Criteria	Answer	Action	Control Framework
1,2 Do you address unauthorized assets every week?	Yes	Regularly review the measures that are used to protect the organization against unauthorized assets.	Unauthorized asset management process

Item Type	Description	Period	UOM	Qty	Rate	Amount	Annualised
Once-off							
Consulting	Initial consult regarding unauthorised assets	Once-off	Hours	5	100	\$ 500.00	\$ 500.00
Recurring							
Assurance	Verify Monthly	Month	Hours	1.5	100	\$ 150.00	\$ 1,800.00

#2 Inventory and Control of Software Assets L2 (P)

Criteria	Answer	Action	Control Framework
2,1 Do you establish and maintain a software asset inventory of all the licensed software that is installed on the enterprise's assets?	No	Implement and maintain an up-to-date business-approved software asset list of all the licensed software that is installed on the enterprise's assets.	Software asset inventory, Software asset inventory management process

Page 3 of 5

56

■ Answered
■ Unanswered

69%

31%

■ Inherent Risk
■ Residual Risk

Remediation project



Remediation Project

- Use the Risk action plan and the Remediation budget to plan and execute the remediation project.
- Export the Remediation budget as a project to excel, import into any project management service/solution.
- (Roadmap) Integrate to Monday.com for a fully managed project plan to which you can allocate resources, set up timelines, critical path and view Gantt or Kanban Charts.

CX - Remediation Project

Main Table | Gantt | +

New Item | Search | Person | Filter | Sort | Hide

Group Title	Item	Period	Item Type	Matrix	Timeline	Dependent On	Status	People
	Create an inventory that contains all the techno...	Once Off	Assurance	VH16	Aug 17 - 19		Complete	TC
	1. Ensure that the implemented controls and pr...	Weekly	Consulting	VH16	Aug 20 - 21	Create an inventory that contains all the technol...	Working on it	
	2. Create an inventory that contains all the tech...	Once Off	Assurance	VH16	Aug 22 - 24	1. Ensure that the implemented controls and proces...	Not Started	
	3. Ensure that the implemented controls and pr...	Weekly	Consulting	VH16	Aug 25 - 26	2. Create an inventory that contains all the technol...	Not Started	
	4. Create an inventory that contains all the tech...	Once Off	Assurance	VH16	Sep 20 - 21	3. Ensure that the implemented controls and proces...	Not Started	
	5. Ensure that the implemented controls and pr...	Weekly	Consulting	VH16	Sep 22 - 23	4. Create an inventory that contains all the technol...	Not Started	
	+ Add Item							

CX - Remediation Project

Main Table | Gantt | Kanban | +

New Item | Search | Person | Filter | Sort

Not Started / 4

- 2. Create an inventory that contains all the technology assets with the potential to store or process ...
- 3. Ensure that the implemented controls and processes that are used to respond to unauthorized ...
- 4. Create an inventory that contains all the technology assets with the potential to store or process ...
- 5. Ensure that the implemented controls and processes that are used to respond to unauthorized ...

+ Add Item

Working on it / 1

- 1. Ensure that the implemented controls and processes that are used to respond to unauthorized ...

+ Add Item

Complete / 1

- Create an inventory that contains all the technology assets with the potential to ...

+ Add Item

Empty / 0

+ Add Item

Gantt

Baseline | Auto FR | Days | - | + | ...

Week 33 Aug 15 - Aug 21 | Week 34 Aug 22 - Aug 28 | Week 35 Aug 29 - Sep 4

Group Title

Aug 17 - Sep 21 ● 38 days

Create an inventory that contain... Aug 17 - 19

1. Ensure that the implemented... Aug 20 - 21

2. Create an inventory that conta... Aug 22 - 24

3. Ensure that the implemented... Aug 25 - 26

4. Create an inventory that conta... Sep 20 - 21

5. Ensure that the implemented... Sep 22 - 23

202008 Project export to Monday.com

Metric	Control No	Criteria No	Criteria	Answer	Risk	Action
VH16	1	1.1	Do you establish and maintain a detailed enterprise asset inventory?	Not all technology assets with the potential to store or process information are known to the business.	Not knowing all the technology assets with the potential to store or process information, whether connected to the network or not, will introduce risk to the business's data and security incident.	Create an inventory that contains all the technology assets with the potential to store or process information, whether these technology assets are connected to the network or not.
VH16	1	1.2	Do you address unauthorized assets every week?	Unauthorized assets are not effectively handled.	Unauthorized assets increase the risk of attacks, for example, data breaches or the introduction of malware, and must be addressed in a timely manner.	Ensure that the implemented controls and processes that are used to respond to unauthorized assets are enforced weekly for all the unauthorized assets.

Ongoing Monitoring



Ongoing Monitoring

Manage ongoing cyber security health.

This includes:

- RMM – Remote Monitoring and Management.
- Endpoint management.
- Network device management.
- Patch Management.
- Server Management.
- User management.
- Professional Services.
- And many others.

Plan for your next
Cyber Security Assessment.



3rd Party Risk Management



3rd Party Risk*

- Create periodic assessments for 3rd parties.
- These can be using any framework in the system.
- Send directly to 3rd party.
- 3rd Party can complete the assessment and add unlimited evidence of activity per criteria.
- 3rd Party marks as completed.
- Assessment is reviewed, marked as Adequate OR Requiring remediation.
- Full report of each 3rd Party assessment is available.
- Each assessment can be compared with other 3rd Party Assessments.

* Note: Only available with company subscription.

Tai One Q4 2022 01 Nov 2022 **CIS 8.0 (IG1)**

Assessment SET ASSESSMENT TO COMPLETE

#1 Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Ref	Criteria	Responses
1,1	Do you establish and maintain a detailed enterprise asset inventory?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>
1,2	Do you address unauthorized assets every week?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>

#2 Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Ref	Criteria	Responses
2,1	Do you establish and maintain a software asset inventory of all the licensed software that is installed on the enterprise's assets?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>
2,2	Do you ensure that only authorized software, that is currently supported by the vendor, is listed in the software asset inventory, for all enterprise assets?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>
2,3	Do you ensure that unauthorized software is either removed from enterprise assets or documented as an exception, regularly?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>

#3 Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Ref	Criteria	Responses
3,1	Do you establish and maintain a data management process?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>
3,2	Do you establish and maintain a data inventory, based on the enterprise's data management process?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>
3,3	Do you configure data access control lists (ACLs) based on a user's need to know and apply them to local and remote file systems, databases, and applications?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>
3,4	Do you enforce data retention according to the enterprise's data management process, with minimum and maximum timelines?	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>
3,5	Do you securely dispose of data as outlined in the enterprise's data management process, taking into consideration the data's	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="checkbox"/>

Evidence of Activity 1,1

Enter evidence of activity

Attach File

Add Evidence Of Activity

Assessment: Current
Date: 04 Nov 2022 09:56
By: Tai PrivIQ
This is evidence of activity

56 Answered / 43 Unanswered

57% Inherent Risk / 43% Residual Risk

The frameworks we use - CIS & NIST

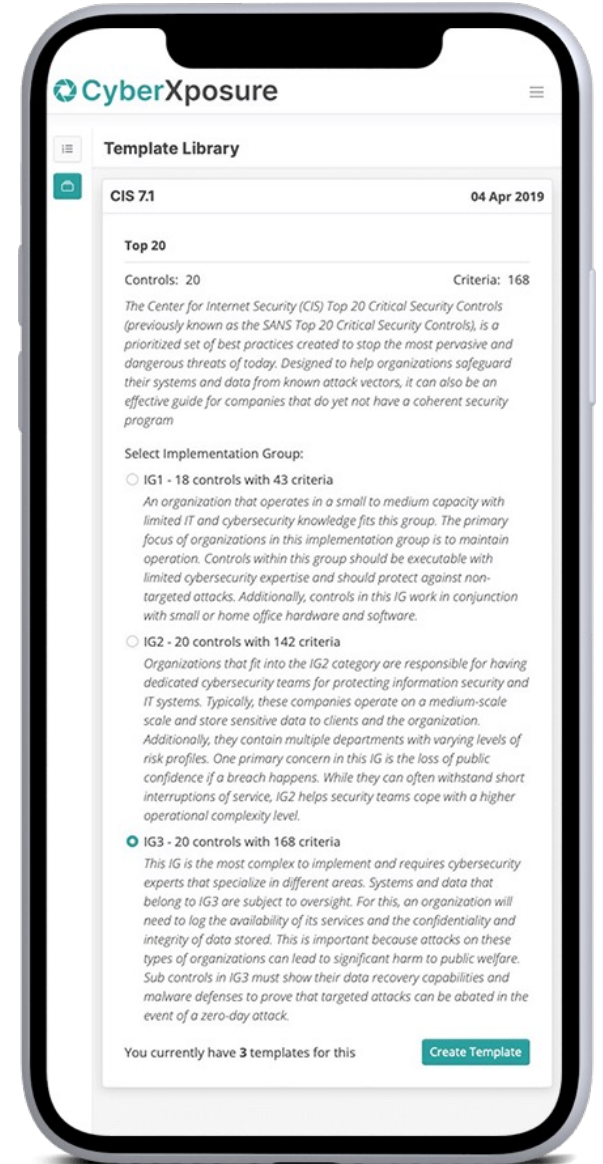




“Developed by the Center for Internet Security (CIS), the CIS Critical Security Controls are a prescriptive, prioritized set of cybersecurity best practices and defensive actions that can help prevent the most pervasive and dangerous attacks and support compliance in a multi-framework era”.

“The CIS Controls are a general set of recommended practices for securing a wide range of systems and devices, whereas CIS Benchmarks are guidelines for hardening specific operating systems, middleware, software applications, and network devices” – www.cisecurity.org

We offer CIS 8.0 IG1, IG2, IG3.



NIST

“NIST Cybersecurity Framework is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology based on existing standards, guidelines, and practices”.

We offer NIST CSF 1.1

Profile 1, 2, 3, 4. These profiles are pre-defined based on the size and security posture of the organization.



Thank you.

For more information and to contact us, please visit:

Website: <https://www.cyberxposure.com>

