CyberXposure

Product Overview

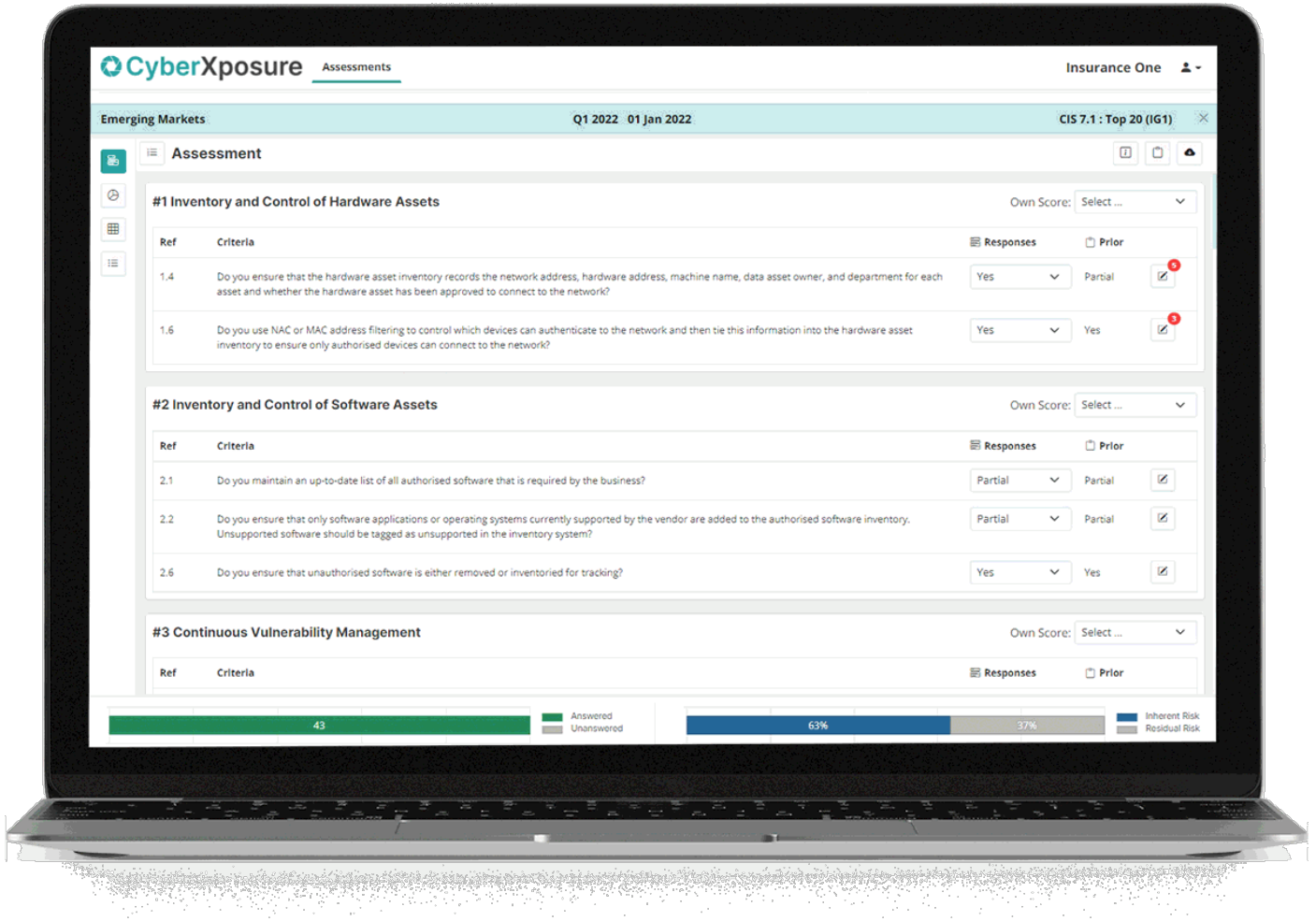
https://www.cyberxposure.com

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



CyberXposure

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.

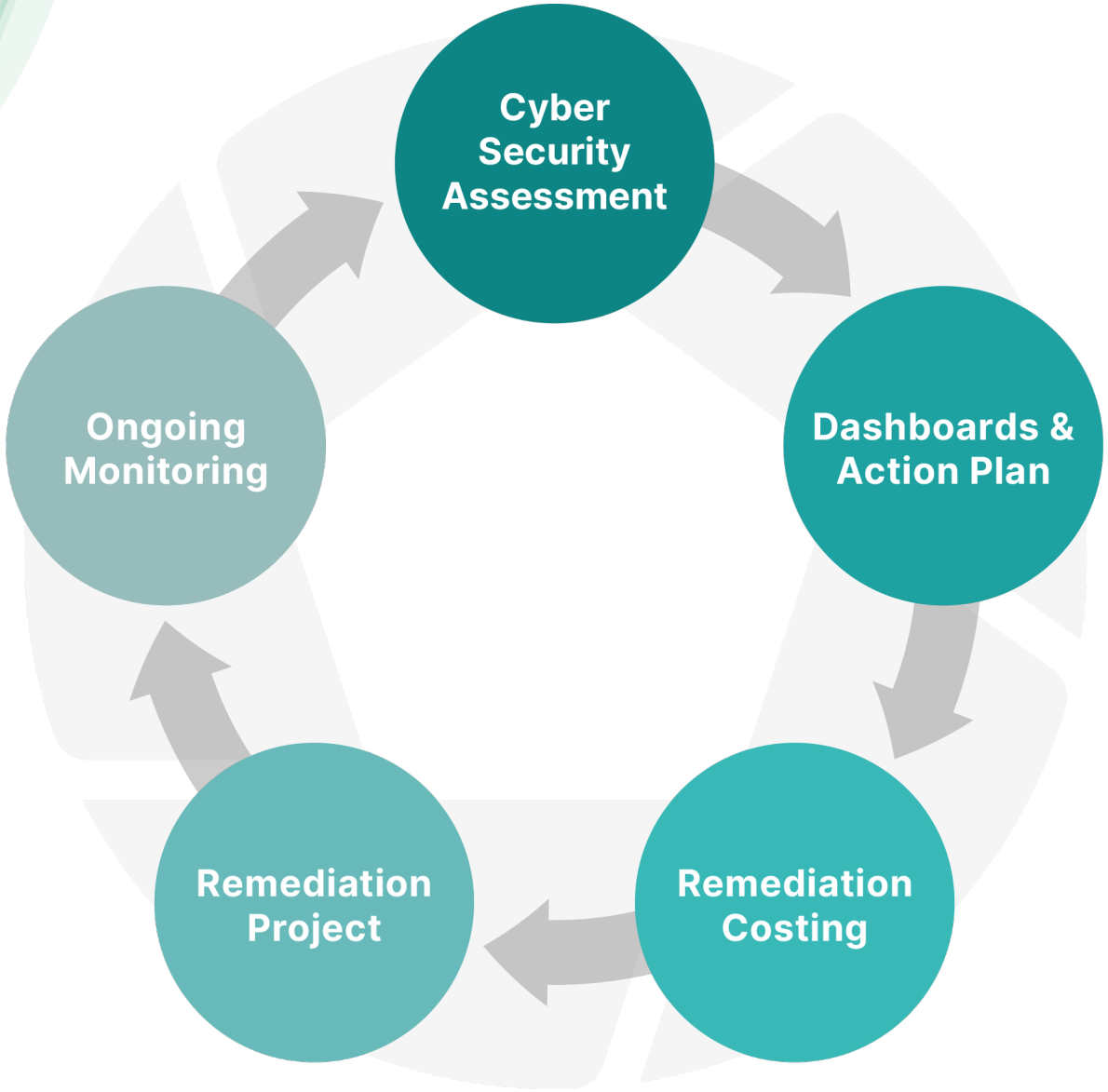
Work collaboratively

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.

CyberXposure

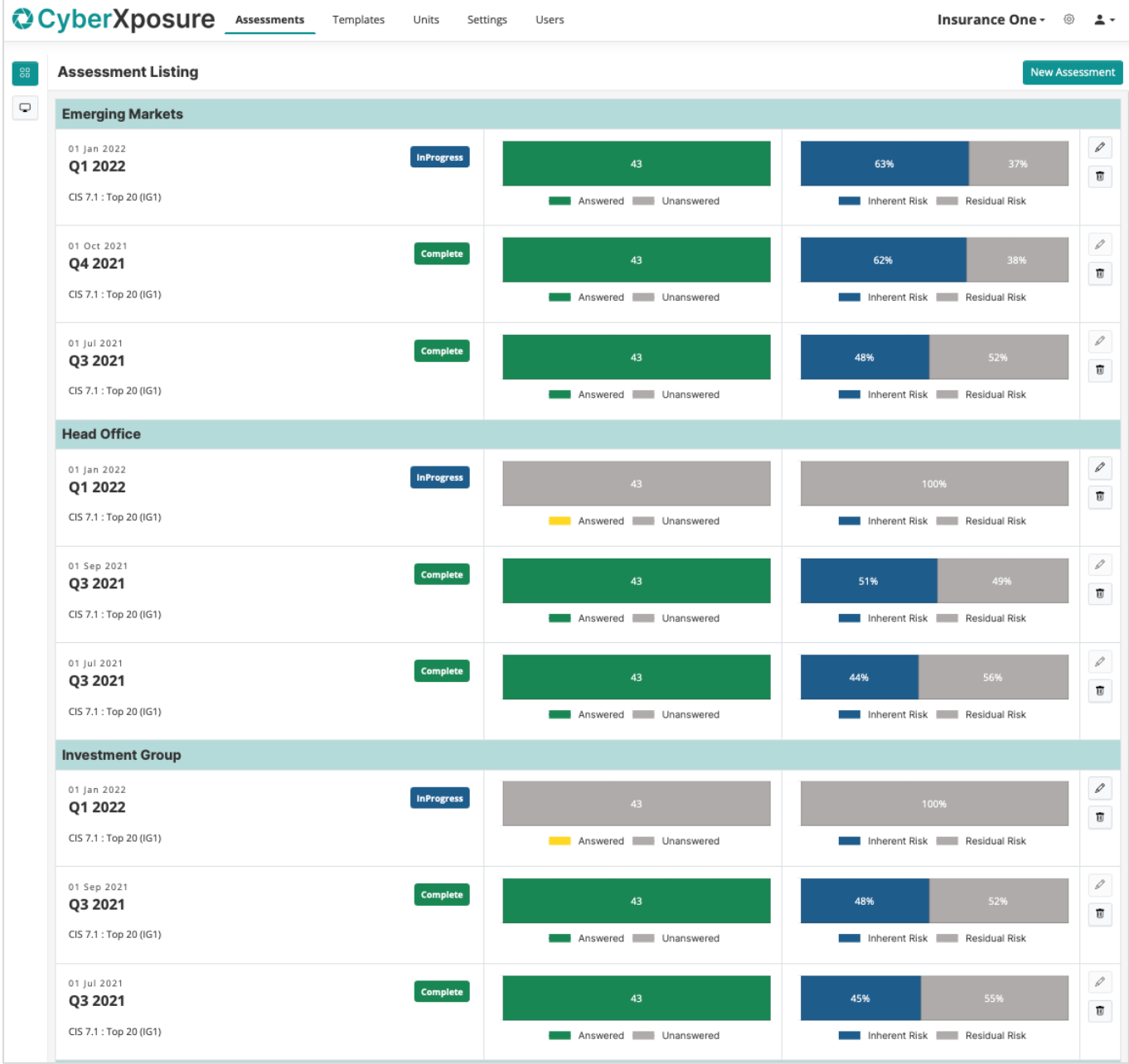


The CyberXposure Cycle

Cyber Security Assessments

Assessments

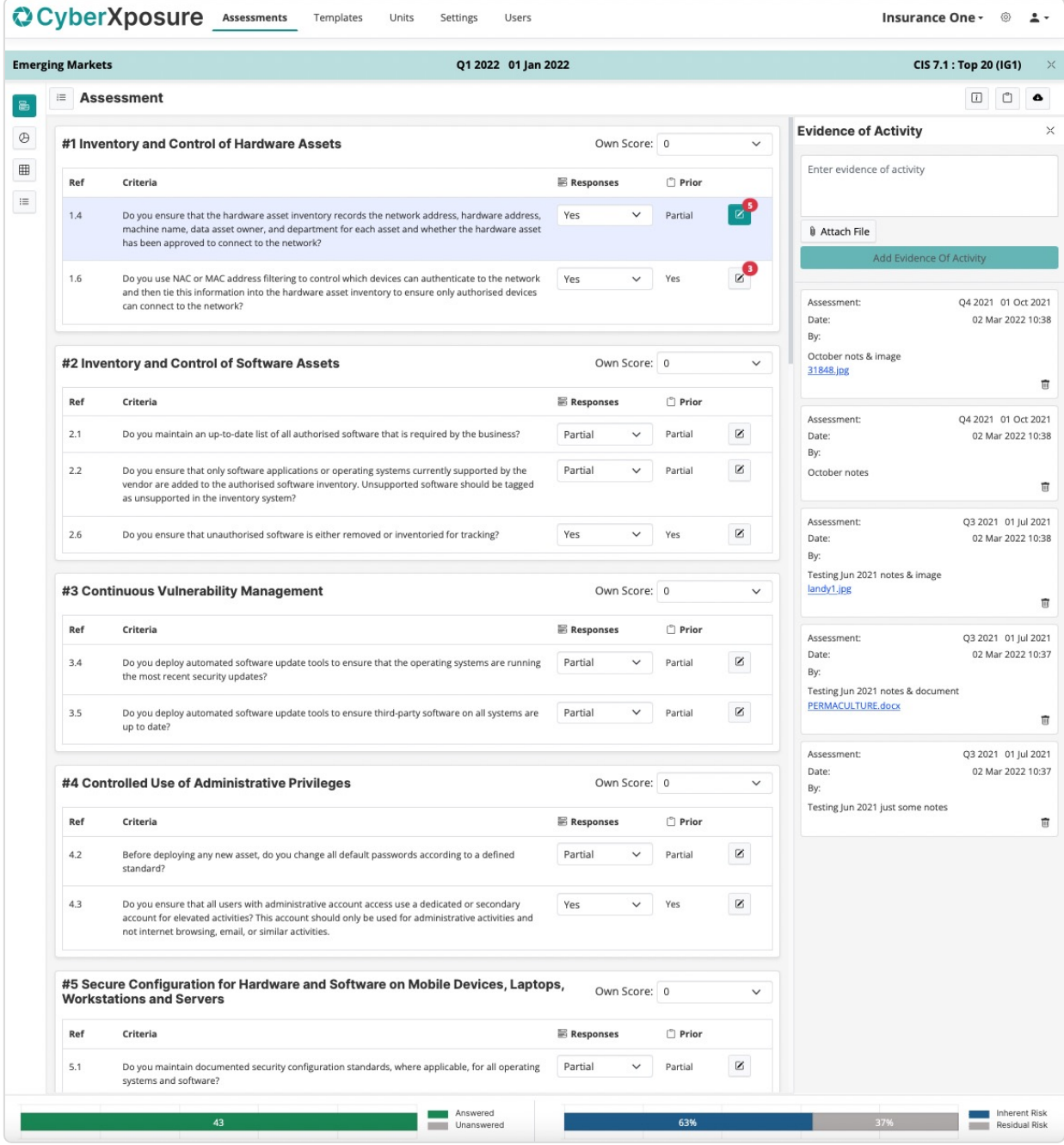
- Set up how often you wish to do reviews - monthly, quarterly, bi-annually or annually.
- Define your team with relevant permissions for access.
- Using our assessment templates, simply determine the templates and sub-sets of templates you want to use (CIS 8.0 IG1,2,3 / NIST CSF 1.1 Profile1,2,3,4).
- 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

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.



CyberXposure

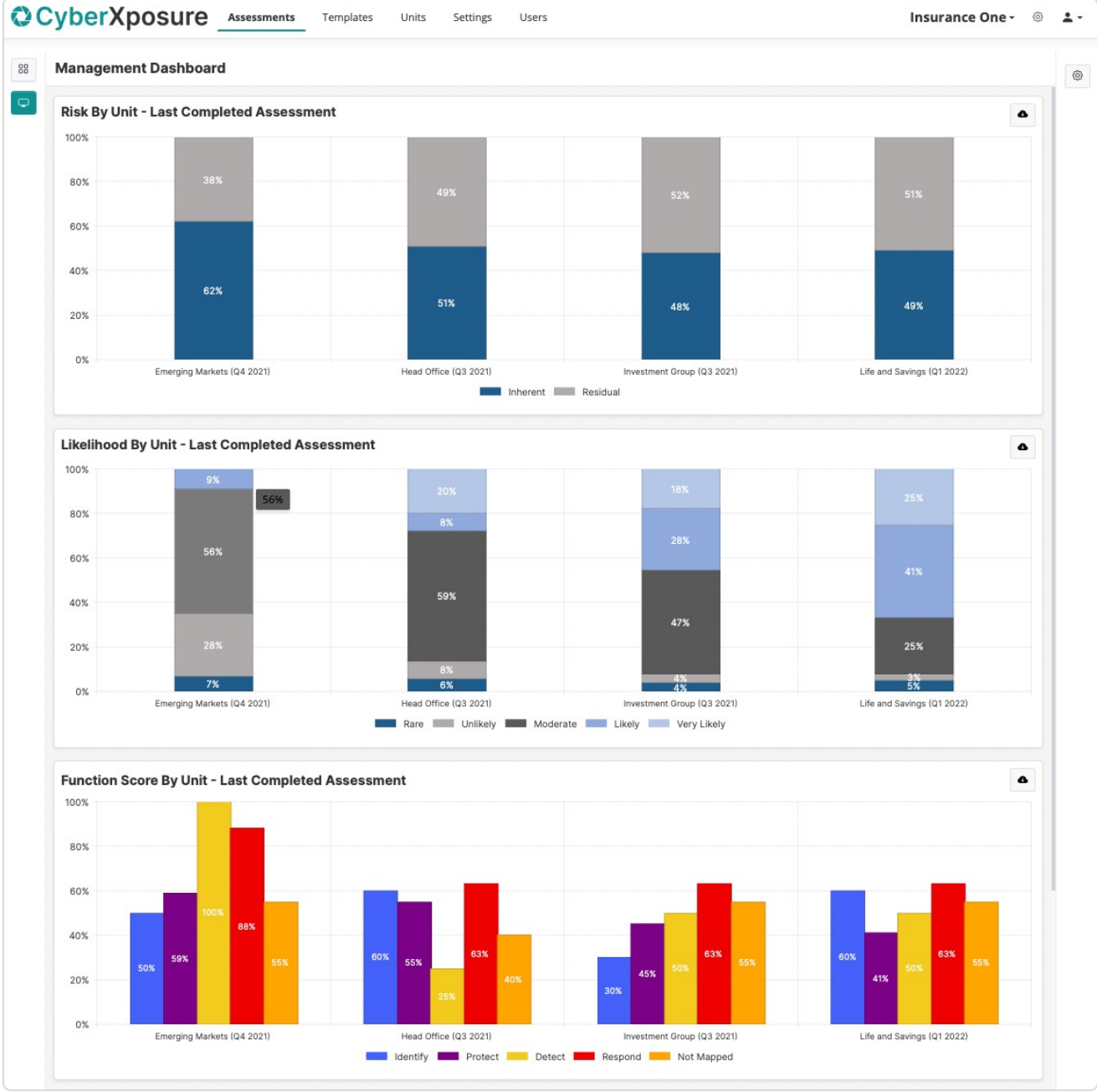
Dashboards and action plan

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:

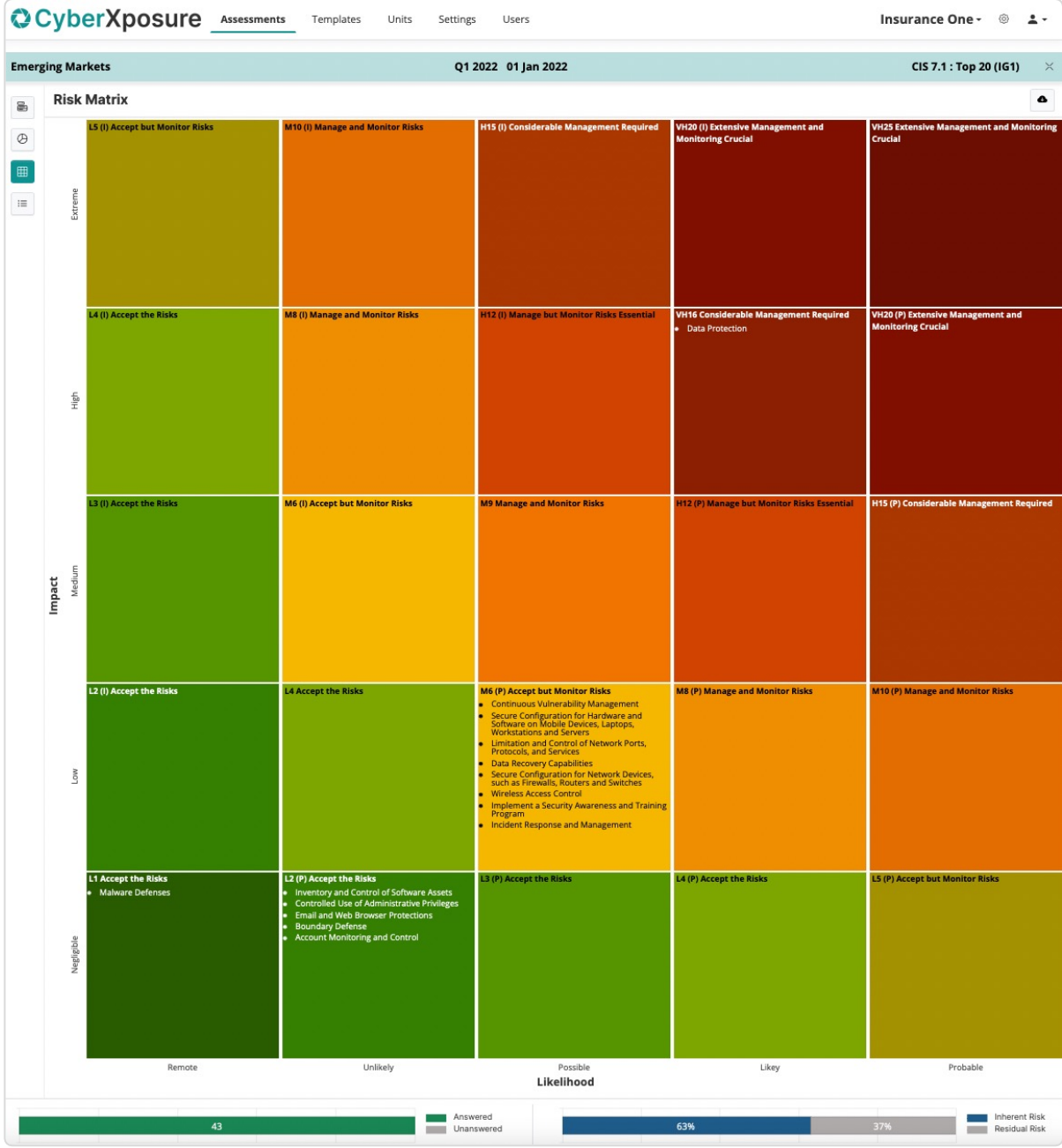
- Inherent vs Residual Risk by Unit.
- Event likelihood by Unit.
- NIST Function score by Unit (Both for NIST and CIS based frameworks).
- Residual Risk by Unit across time.
- These are key to being able to report on progress (or lack thereof) to the organisation's leaders as required.



CyberXposure

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.



CyberXposure

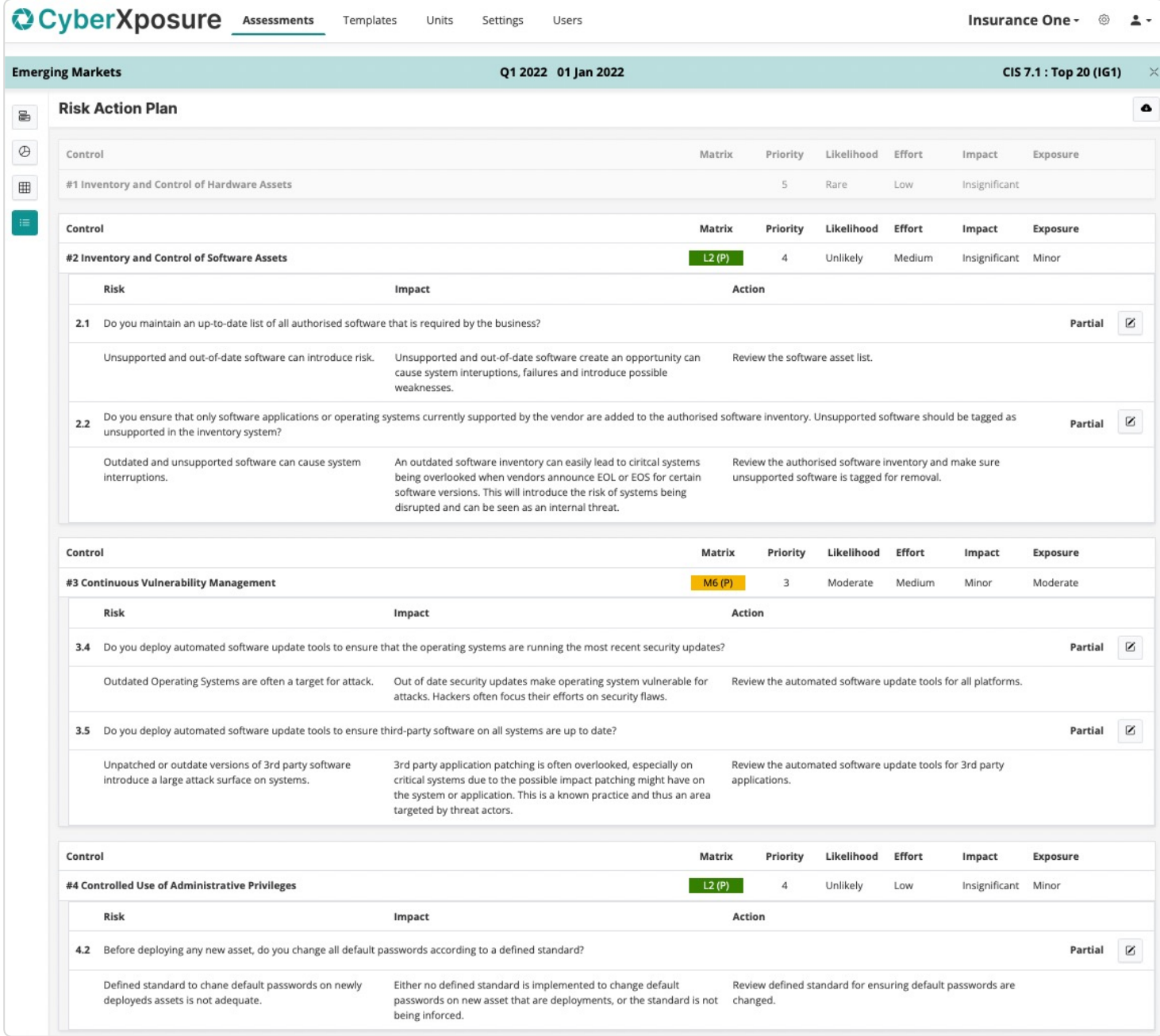
Assessment Dashboard

- 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.

CyberXposure

Risk Action Plan

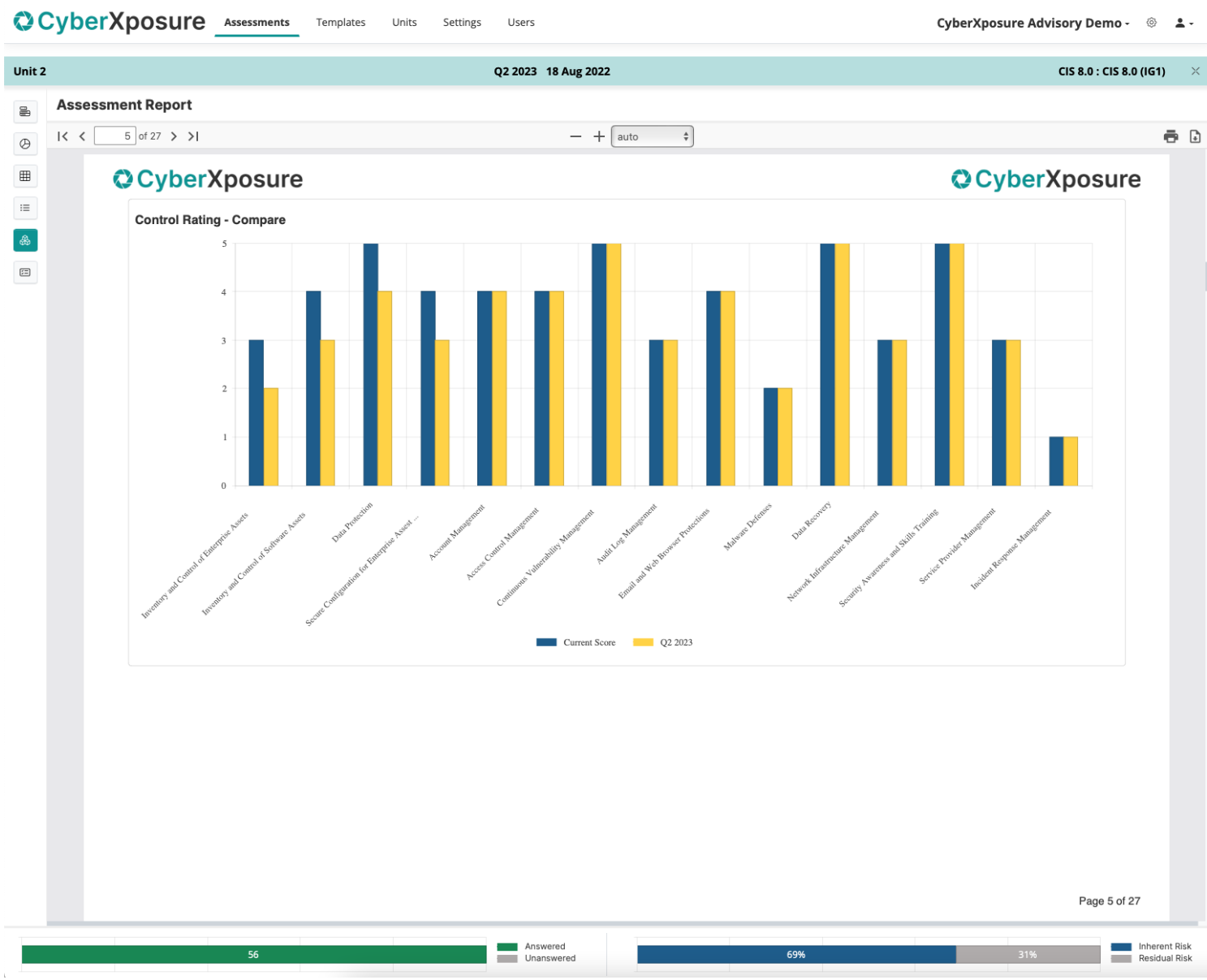
- When an assessment is in progress, we dynamically create a Risk Action Plan. This tells you exactly what actions need to be performed, all graded by KPI's, in order to move from a non-conforming to conforming position.
- When an assessment is completed, it may be that not all risk areas have been resolved. 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

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.

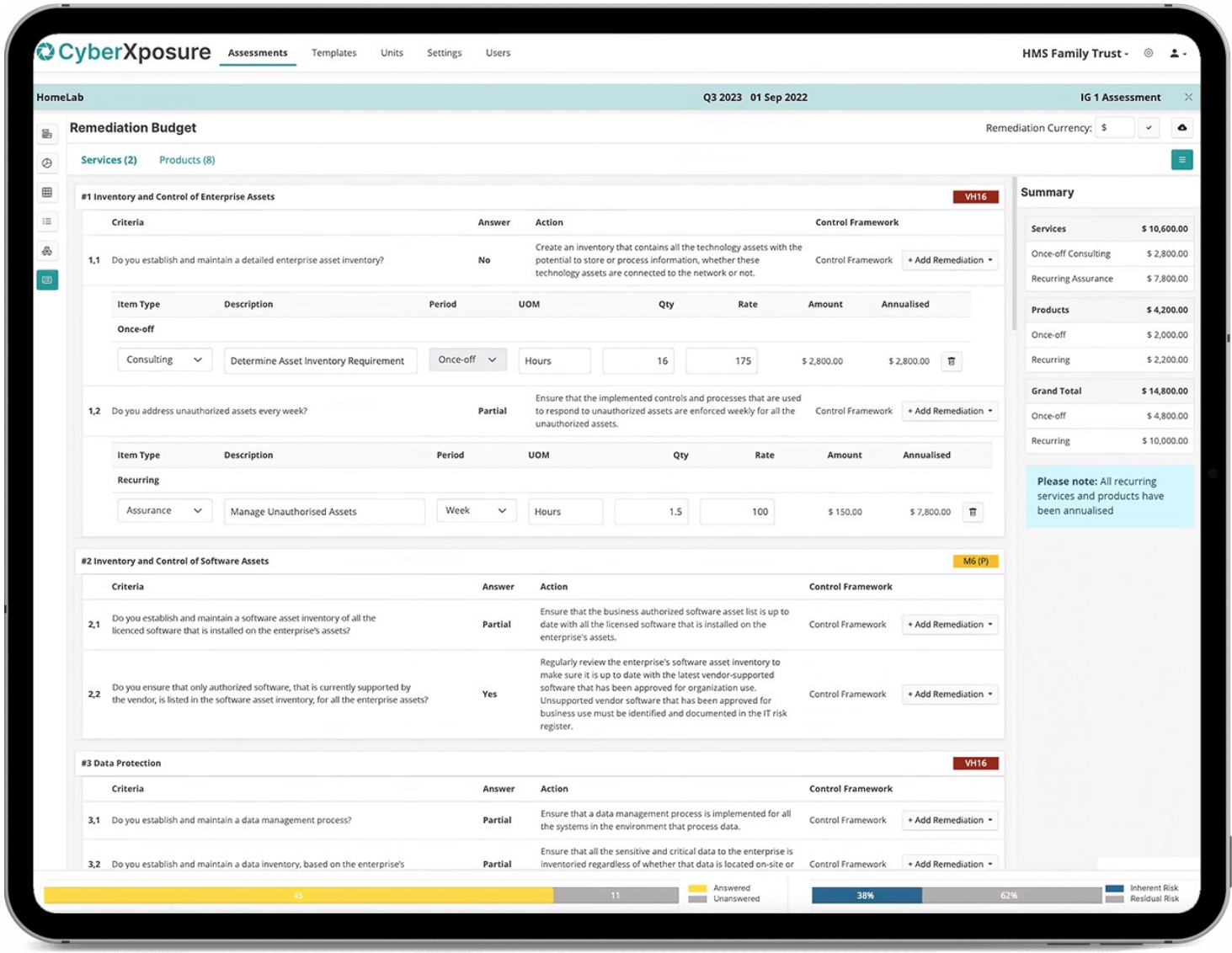


CyberXposure

Remediation costing

Remediation Costing

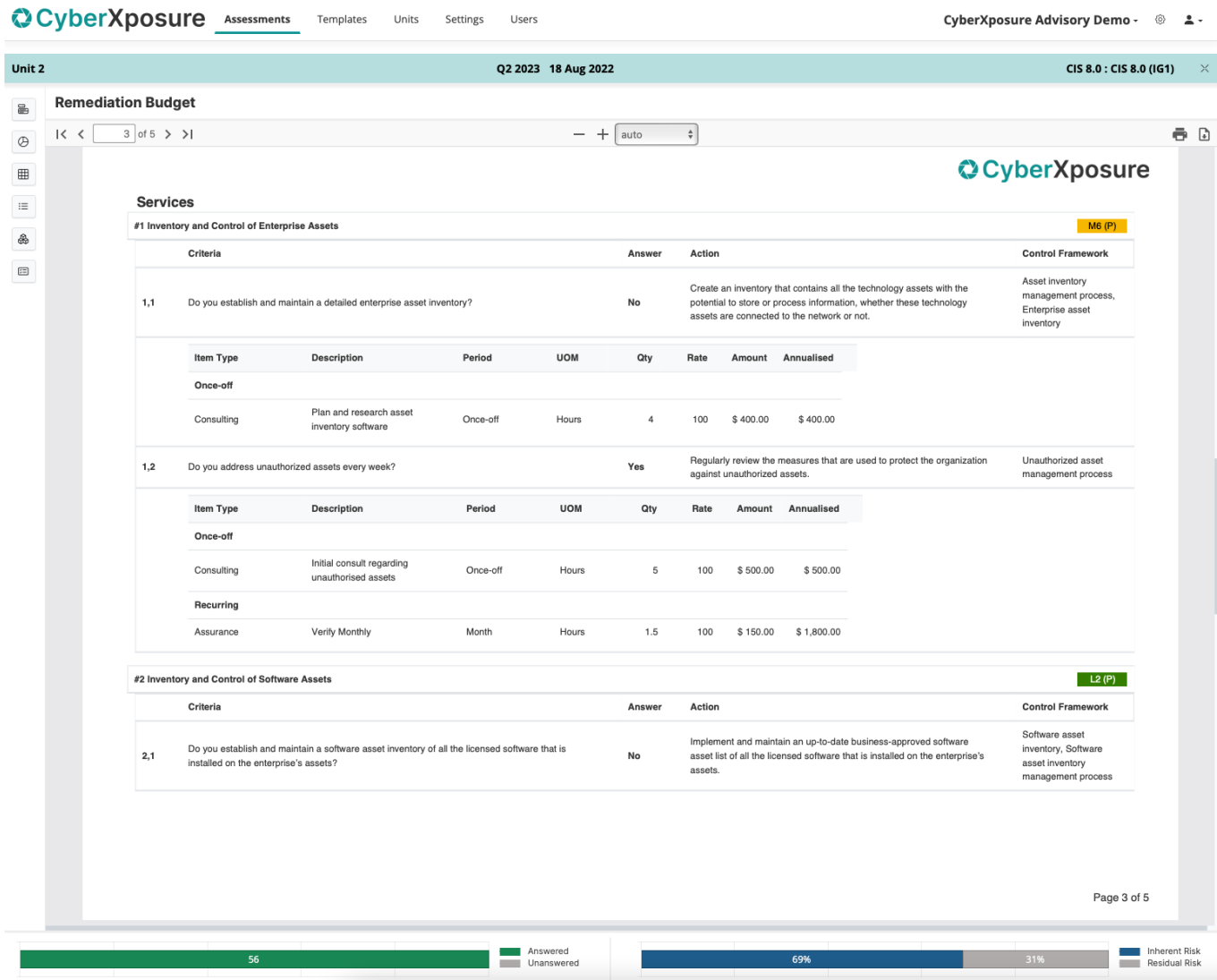
- This is a critical task, how to budget / quote your client on their remediation. The best way is based on the assessment. We offer a full budget/quotation methodology based on risk and impact.
- Build a full remediation cost model with services and products to enable a prioritised and executable plan 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.



CyberXposure

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.

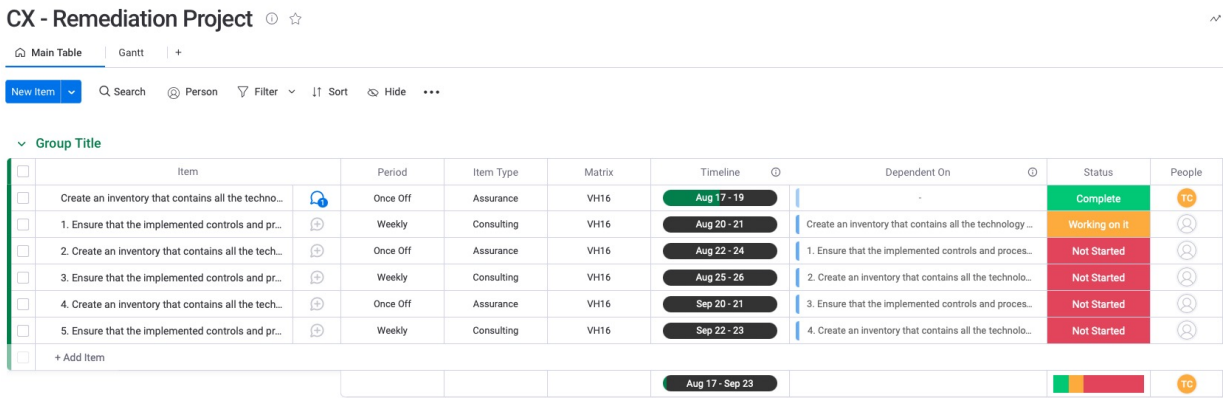


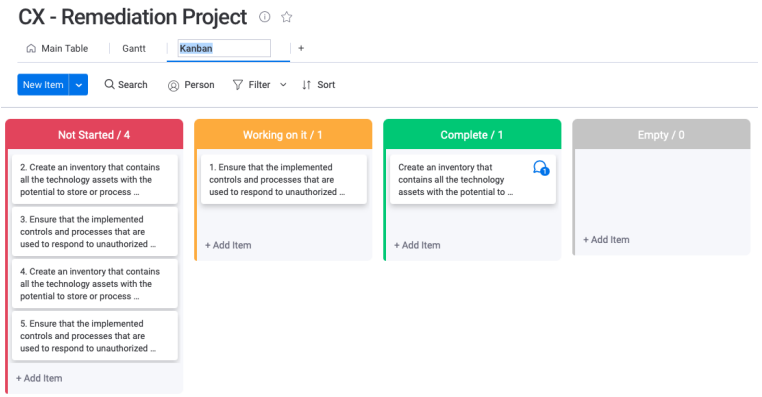
CyberXposure

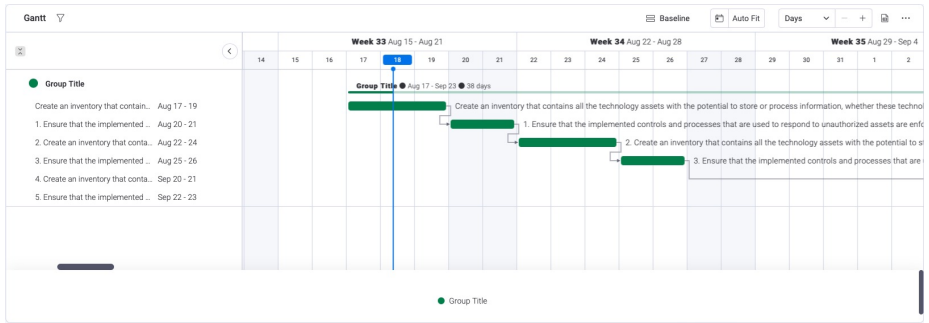
Remediation project

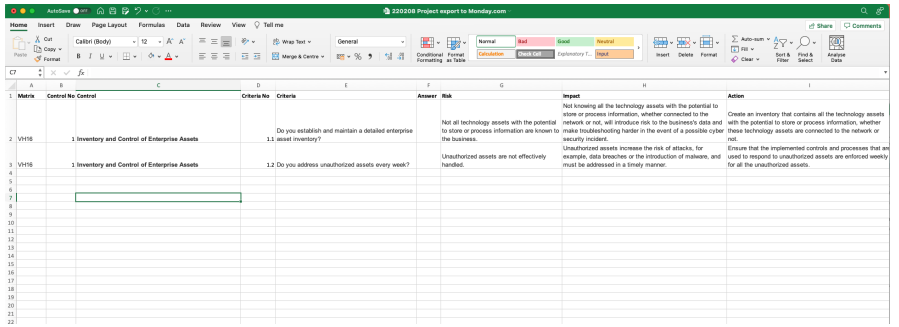
Remediation Project

- 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.









CyberXposure

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.

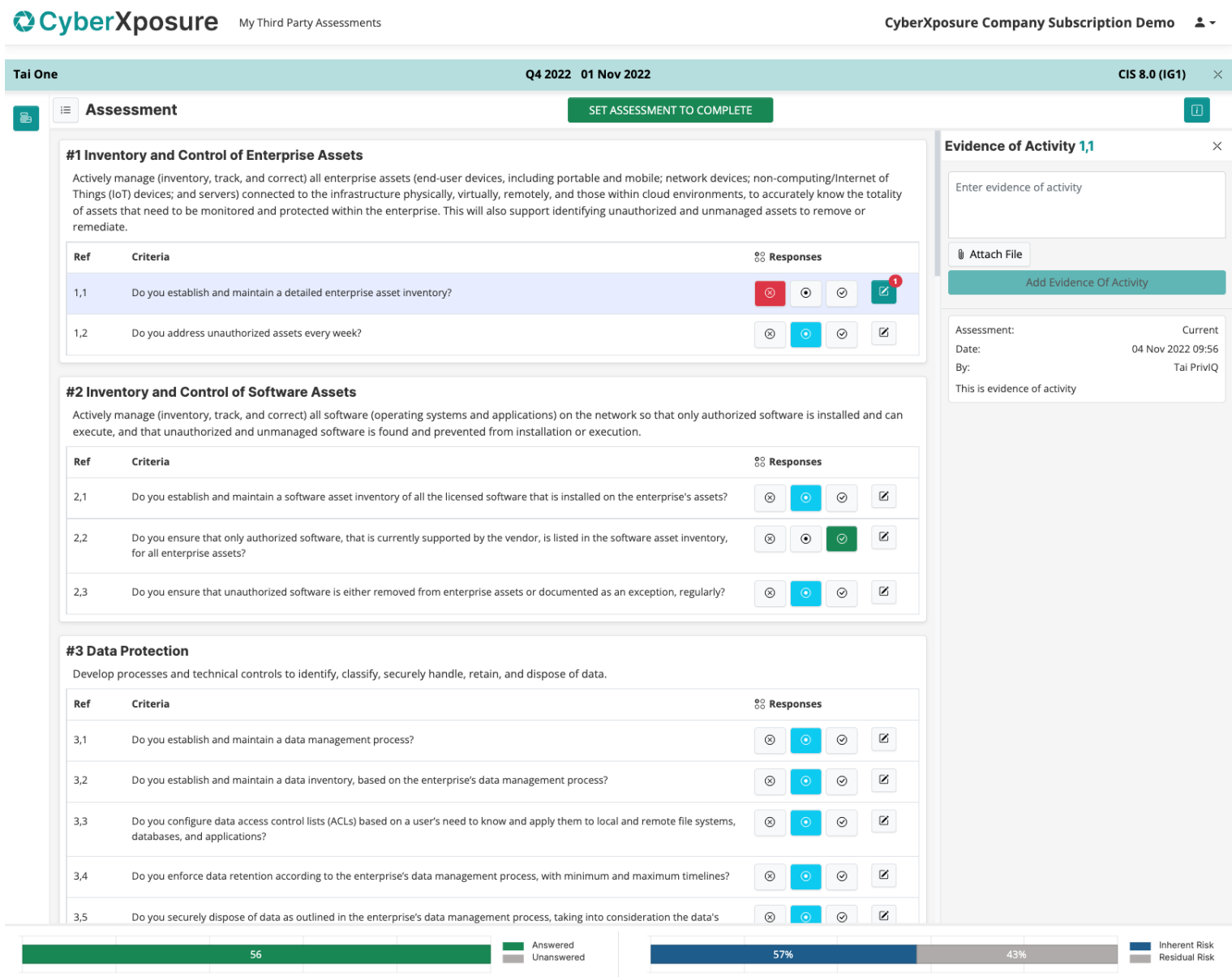
Plan for your next
Cyber Security Assessment.

CyberXposure

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.

CyberXposure

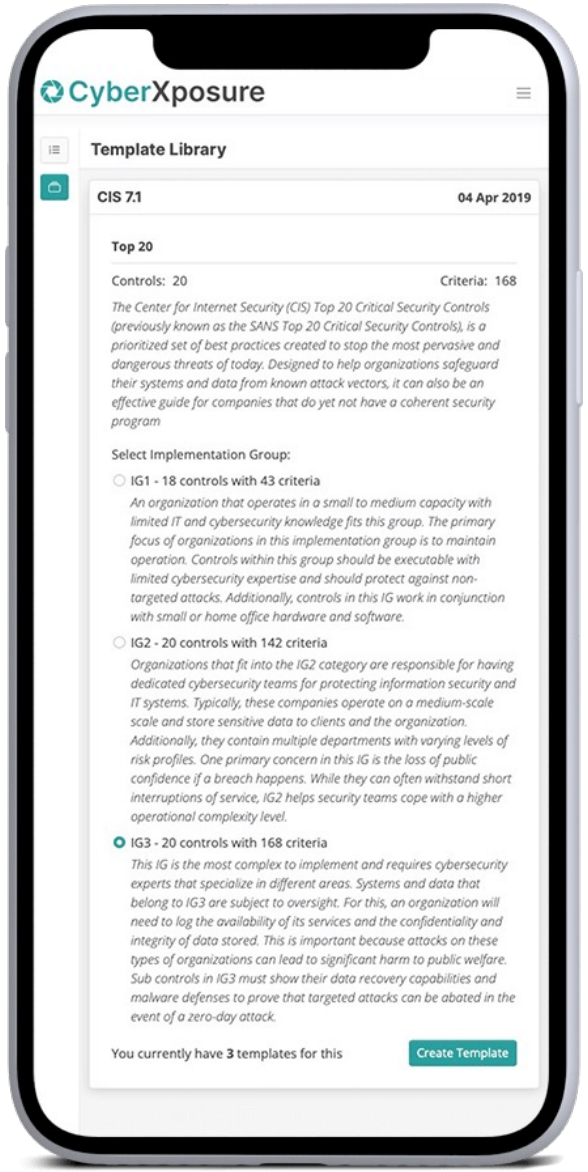
The frameworks we use - CIS & NIST

CIS

“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