Cyber Quant

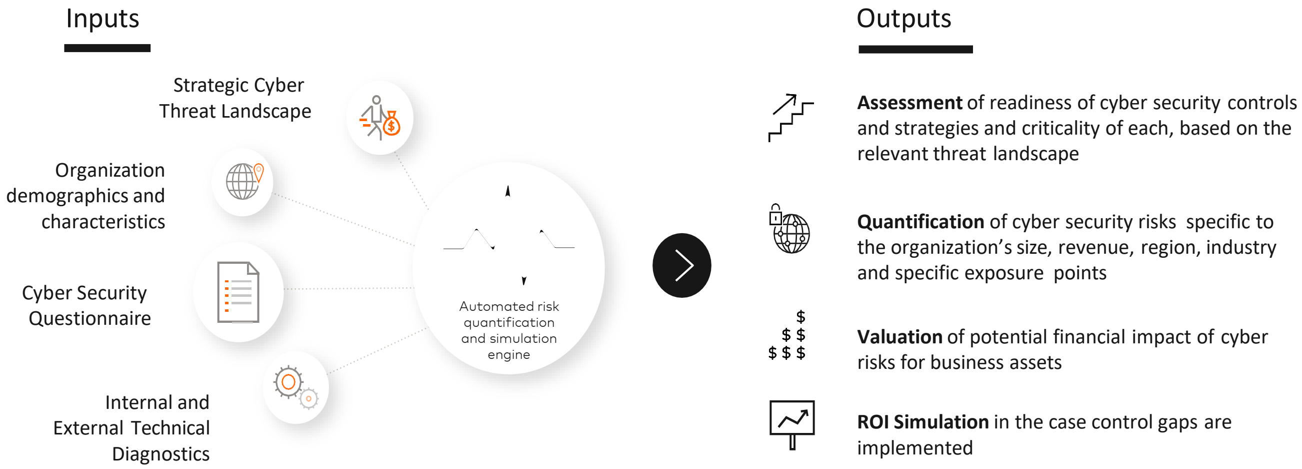
Mastercard Cyber Quant FAQ

JUNE 2024

General Information

Q: What is Mastercard Cyber Quant?

A: Mastercard Cyber Quant is a cybersecurity risk assessment SaaS platform. It enables an organization to understand their cyber maturity and risk posture, and to construct the strategy for addressing the gaps and reducing their cyber risk. The platform starts with questionnaire responses but also integrates with a broad spectrum of technologies to conduct the assessment. In addition, the platform incorporates threat intelligence to bring in a perspective of the who may attack your organization and how.


Inputs
Strategic Cyber Threat Landscape
Organization demographics and characteristics
Cyber Security Questionnaire
Internal and External Technical Diagnostics
Automated risk quantification and simulation engine
Outputs

Assessment of readiness of cyber security controls and strategies and criticality of each, based on the relevant threat landscape

Quantification of cyber security risks specific to the organization's size, revenue, region, industry and specific exposure points

Valuation of potential financial impact of cyber risks for business assets

ROI Simulation in the case control gaps are implemented

Cyber Quant helps organizations conduct a cyber risk assessment efficiently and effectively. Underlying the Cyber Quant engine are industry standards, frameworks, best practices, and Mastercard's proprietary analytics and risk calculation capabilities. With Cyber Quant an organization can conduct a quick assessment in less than an hour, to a deeper assessment in a few weeks (not months or years)!

Q: What is the foundation of the Cyber Quant questionnaires?

A: All security standards and frameworks have similar underlying principles of protecting confidentiality, integrity, and availability of data. Cyber Quant incorporates inputs from various standards to define the Cyber Quant Security Framework. Given the variety of needs organizations may have, the platform offers multiple levels of assessments based on questionnaires using this framework. In addition, the platform also offers the ability to conduct maturity assessments for standards such as NIST CSF 1.0 /1.1, ISO-27002:2022, PCI DSS 4.0, CIS Controls, HIPAA, and CRI.

Platform Overview

Q: Is Cyber Quant a SaaS-based tool? What is required for deployment?

A: Yes, Cyber Quant is a SaaS platform hosted on Mastercard's AWS instance. Using the CIS license product for input, the platform runs scripts on servers, network devices, or all the databases itself. We're not running scanning tools. The scripts identify how we can further harden the configuration files of the systems we are assessing.

Q: Is Cyber Quant SOC II or ISO certified?
A: Cyber Quant is not SOC 2 or ISO certified – we are currently working towards this effort.

Q: Can Cyber Quant do benchmark against multiple industry standards through a single assessment?
A: Yes, we can do industry benchmarking. We have the most data in financial services, but we can accommodate other industries that meet your client's needs.

Questionnaires Types, Frameworks / Standards

Q: Does Cyber Quant use a questionnaire, and is it based on any standard frameworks?
A: Based on Mastercard Cyber Quant Security Framework, Cyber Quant offers multiple questionnaires to help an organization conduct various levels of risk and maturity assessments. Starting from 15 questions and going over 500, the questionnaires offer flexibility centered on the level of depth the organization wants to evaluate. In addition, the organization can also conduct maturity assessments for standards such as NIST CSF 1.0 /1.1, ISO-27002:2022, PCI DSS 4.0, CIS Controls, HIPAA, CRI, and other common frameworks.

Q: Does Cyber Quant have support for FFIEC standards?
A: The Mastercard Cyber Quant team continually adds coverage for new security standards and frameworks based on relevance to cybersecurity trends and based on customer needs. If a particular standard or framework interests you, please provide your business case to the Mastercard representative. We will assess and prioritize your request accordingly.

Q: Can multiple questionnaires be generated into one dashboard to view the results, or does each questionnaire receives its own dashboard.
A: This is possible; in an assessment, environment 1 can have a CQ Essentials 47 questionnaire, while environment 2 could have an Essentials 500+ questionnaire. The resulting assessment is a combination of all of it.

Q: Can you show the mapping of frameworks or progress against each framework in a dashboard?
A: The dashboard can show the results of a framework assessment and compare it with other frameworks (maturity levels). We also have a report to show this comparison.

Technology Assessments & Integrations

Q: Which technologies does Cyber Quant integrate/support?
A: Validation is achieved by importing technical configuration files from +100 technologies and comparing them against maturity indicators based on community and industry best practices. To ensure the security of your organization's data, processing activities are done on the premises.

Furthermore, to ensure greater visibility of various information technologies, the CIS-CAT Pro Assessor has been incorporated into CyMA, along with a license to utilize it. CyMA leverages the reports of CIS-CAT Pro in its maturity analysis to quickly and efficiently scan any system in the network against various CIS benchmarks.

- ✓ AWS
- ✓ Microsoft Cloud Security
- ✓ Check Point
- ✓ CrowdStrike
- ✓ FortiGate, Palo Alto
- ✓ McAfee
- ✓ Palo Alto
- ✓ Okta
- ✓ Symantec
- ✓ Windows Enterprise
- ✓ Windows Server
- ✓ CentOS Linux
- ✓ Cisco IOS
- ✓ Google Chrome
- ✓ Microsoft Edge
- ✓ Microsoft Exchange
- ✓ Oracle MySQL Enterprise Edition
- ✓ Google Kubernetes Engine
- ✓ Amazon Elastic Kubernetes Service
- ✓ Kubernetes
- ✓ VMWare

For more detailed information about supported technologies, please consult the Cyber Quant - Supported Technologies article on our Knowledge base website

Q: What license does an organization need to use CIS CAT Pro?
A: CIS CAT Pro is included in the Cyber Quant Essential assessment. If the organization wants to continue using CIS CAT Pro on an ongoing basis after the end of the CQ assessment, then the client will need to subscribe to CIS directly through CIS. Upon the end of the assessment, and if the client is not a CIS member, then the CIS CAT Pro application must be uninstalled.

Q: Who has access to the CIS CAT Pro assessment results?
A: The user/ the users' system administrator is the only one who has access to the CIS CAT Pro results. The tool installation, the running of the benchmark assessment on any of your IT systems, and the visibility of the output reports are all managed by the user/user system administrator. The user or users' system administrator uses Cyber Quant's CyMA application to import data from these reports. Cyber Quant extracts only configuration compatibility information, which is not identifiable information about your systems.

Q: What Mastercard solutions are integrated with Cyber Quant?
A: Risk Recon & Cyber Front

Technology Assessments & Integrations

Q: Will the Cyber Quant and RiskRecon dashboards be integrated into one uniform dashboard that gives a CISO one view inside-out/outside-in and shows the ROI where to invest their money?
A: Today they are separate stand-alone platforms; they can be used in an integrated fashion. You can plug in information with the Cyber Quant portal from RiskRecon and run ROI calculations, simulations, from RiskRecon directly. However, the dashboards are not directly integrated.

Q: Are there additional costs associated with integrating the results of Risk Recon scans into Cyber Quant?
A: As long as the client has the license for both solutions, there is no additional fee for importing data from RiskRecon to Cyber Quant.

Q: Do you have issues sourcing client information from the integrated tools?
A: The integration effort is relatively straightforward, and each integration is supported with guidance documents. The platform offers passive and active technical validation capabilities, including simple URL or domain entries, API integrations, and the industry-recognized CIS CAT Pro toolset. As we guide the customer on the importance of technical validation, the value is recognized quickly.

Cyber Quant Assessment Journey

Q: What are Cyber Quant's implementation options?
A: The Cyber Quant platform empowers and suits large and small organizations by offering several assessment implementation options. For more information, please review our Knowledge Base's Cyber Quant—Implementation Options Article.

Q: What is the Cyber Quant framework built on?
A: The Cyber Quant Framework was created based on security standards such as NIST CSF, ISO 27002:2022, PCI DSS 4, CIS controls, HIPAA, etc. We extracted the core security requirements from these standards and unified them into one questionnaire.

Q: What are the supported standards by Cyber Quant?
A: Cyber Quant allows users to do specialized maturity assessments against many security standards, regulations, and frameworks (referred to as sources for simplicity) without going through the entire risk assessment process with threat landscapes and organization definitions. To get the full list and details of the supported standards and frameworks, please review Knowledge Base's Cyber Quant - Standards, Regulations, and Frameworks Article

Q: How often should I run a risk assessment?
A: We recommend that the organizations refresh their results quarterly. Quarterly and perhaps monthly assessments will help the organization track the progress and impact on the cyber risk score due to various changes the organization is making to their environment (cybersecurity tools, policies, processes, IT changes, acquisition of an organization/systems integration, etc.), and due to the everchanging threat landscape (keeping an eye on emerging threats, changes due to geopolitical events, etc.). With Cyber Quant, the quarterly refresh of the assessment is easier as previous responses are carried forward, so the assessor only updates the inputs, not start from scratch!

Q: What is the Cyber Quant Lite project experience for the customer (organization completing the assessment)?
A: The customer completes the Cyber Quant Lite assessment online by connecting to the Cyber Quant SaaS platform. Thus, the customer needs to have internet connectivity to complete this assessment. The customer journey entails the customer logging into the platform based on credentials we will email to them. Once logged in, the customer will:

1. Fill out basic information about their organization about the size and location of the company
2. Respond to a questionnaire ranging from 15 – 50 questions (dependent on the scope of assessment as defined by the sponsoring organization)
3. Select and run passive technical checks to evaluate cybersecurity settings for the website, email server, DNS, operating system, and browser. (dependent on the scope of assessment as defined by the sponsoring organization)
4. Review the results / download the results

The journey from start to finish takes about 1 hour to complete.

Cyber Quant Assessment Journey

Q: What is the Cyber Quant Essentials project experience for the customer (organization completing the assessment)?

A: The customer completes the Cyber Quant Essentials assessment online by connecting to the Cyber Quant SaaS platform and through two applications (Control Maturity Analysis Tool - CyMA, and CIS-CAT Pro Tool, both included with Cyber Quant Subscription) installed on the customer's premises. The customer could need administrator permissions (depending on customer infrastructure) to install the applications and run certain queries on their IT environment.

The customer journey entails the customer logging into the platform based on credentials we will email to them. Once logged in, the customer will:

1. Fill out basic information about their organization about the size and location of the company
2. Respond to a questionnaire ranging from 50 – 500+ questions (dependent on the scope of assessment as defined by the sponsoring organization)
3. Select and run passive technical checks to evaluate cybersecurity settings for the website, email server, DNS, operating system, and browser. (dependent on the scope of assessment as defined by the sponsoring organization)
4. Install the Cyber Quant "CyMA" application and the CIS CAT Pro applications
5. Using these 2 applications, collect and process technical configuration information from the organization's IT systems (firewalls, switches, servers, cloud platforms, etc.)
6. Review the results / download the results

The start-to-finish journey can take a few weeks to complete as the organization will coordinate with resources.

Running a Cyber Quant Assessment

Q: Are the comments section (in the questionnaire) removable?
A: Comments can be removed while the assessment remains open. However, you cannot remove the comments once you close the assessment.

Q: Where are uploaded supporting documents stored?
A: Cyber Quant is a SaaS platform based on AWS Cloud Services. All the documents are being uploaded in a unique and encrypted path, created per hub, environment, assessment, and question, into an encrypted bucket per the company's internal number folder in the Cyber Quant AWS environment. The documents are scanned and stored inside the encrypted bucket in a specific company file, ensuring secureness and confidentiality. For a broader description of data handling, please review the Cyber Quant - Technical Solution Briefs Article in our Knowledge Base.

Q: How long are attachments stored for or accessible?
A: The attachments are stored at the customer's discretion. It means the files and assessments will remain accessible as long as the customer and their assessments are active.

Q: How are attachments removed upon completing an engagement?
A: The customer can remove the attached files at their discretion. If not, the files and assessments will remain accessible as long as the customer and their assessments are active.

Q: What information would be fed and validated for the controls (e.g., its configuration to validate against best practice or monitoring mode)? Does this measure how much of that data exists to determine the value of loss?
A: Each control comprises indicators of maturity gathered from technical assessments of security products and systems (Operating effectiveness) and questionnaires (Design effectiveness) to provide a comprehensive controls assessment. The combination of these two factors calculates the control maturity scores. The data assets are assessed based on industry and the assessor's selections and prioritizations. The group or company's revenue or cost numbers determine the value of the loss.

Q: Can the questionnaire be customized?
A: You can determine the number of questions you want to ask and customize or refine to fit the client's needs. In addition, Cyber Quan has a custom questionnaire capability that allows customers to create their questionnaires.

Q: What are the supported Report export formats?
A: Cyber Quant supports Word and Excel report formats.

Q: Can we download the report (management report/detailed technical report as per requirement after the assessment)?
A: Yes. You can find it on the company assessment page in the HUB by clicking on the 3 dots and selecting reports.

Financial Impact and Risk Calculations

Q: How is financial impact and its relevance to the client calculated?

A: Cyber Quant is a cyber risk quantification solution that leverages strategic threat intelligence with accurate control maturity assessments to systematically identify and quantify the risks to the organization's business assets at multiple degrees of granularity. Two key evaluation outputs are the Risk Score and the Financial Impact range amount for the organization from cyber security-related adverse events.

As you input the demographic information, complete the questionnaire, and upload the technical configuration files, the Cyber Quant platform employs a 9-steps process, starting from understanding the organization to generating insights for remediation and calculating financial impact based on the company's revenues, or associated costs. The following is calculated to find financial impact with relevant analysis being done.

1. Control Maturity
2. Threat Activity Level
3. Probability of Success of Attack Methods
4. Attackers/ Attack Threat Levels
5. Business Asset Risk Level
6. Environment Risk Level
7. Organization Risk Level
8. Remediation Priorities
9. Financial Impact Analysis

Q: What information is used to level the control effectiveness, and how are the results interpreted in the risk assessment?

A: Control effectiveness is related to the control design. Each control comprises indicators of maturity gathered from technical assessments of security products and systems (Operating effectiveness), and questionnaires (Design effectiveness) provide a comprehensive control assessment. The combination of these two factors calculates the Control maturity scores.

Q: Can control scores be manually entered?

A: Control scores can be manually overwritten in the CyMA application.

Cyber Quant Incorporating Threat Intel (Cyber Insights)

Q: How does Data Collection and Processing work in Cyber Insights?
A: Master Workstation is the backend powerhouse of the Cyber Insights tool. It runs automatically in order to provide threat landscape scenarios per industry and geo-political regions to the Cyber Quant Risk Quantification mechanism, in sequential stages:

1. Data Collection: real-time intelligence from thousands of sources in the clear, deep and dark webs (can be added). This includes exclusive access to closed threat actor communities such as forums, marketplaces and invite-only chat groups. Sources are continuously added and curated by the Mastercard team to ensure data quality and integrity.
2. Data Processing: every item collected is automatically reviewed through text analysis to identify tens of thousands of multilingual entities and synonyms in all threat landscape categories. Cyber Insights' entity dictionary contains various depth levels ensuring data can be examined at the lowest resolution to provide accurate context.
3. Statistical Analysis: combines repetitions of the same permutation of entities to create statistics. This expedites the analysis process, minimizes noise and eliminates redundancies.
4. Output: algorithm can then output threat landscape trends and patterns for selected parameters tailored to the organization's circumstances, as well as forecast these for the short-term future.

Q: Why Cyber Insights?
A: Cyber Insights is a tool that collects threat data feeds from thousands of sources and analyzes the intelligence items or "cyber events" within them to create strategic intelligence trends regarding attackers, attack methods, targeted assets, impacted industries and geo-political regions.

Q: How does Cyber Insights work?
A: Cyber Insights uses Master Workstation which is the backend powerhouse of the Cyber Insights tool. It runs automatically in order to provide threat landscape scenarios per industry and geo-political regions to the Cyber Quant Risk Quantification mechanism, in 4 sequential stages.

Q: What period is Cyber Insights' inputs updated in?
A: Cyber Insights' data collection works 24/7 and is constantly ingesting intelligence feeds and processing them to create threat landscape trends. Cyber Insights Analyst Web is currently updating on a daily basis.

Q: Can we define the precision for Cyber Insights' forecast?
A: Cyber Insights' forecasting algorithm is based on statistical regression analysis. When evaluating predicted threat landscape up to one month in advance, Cyber Insights' forecast has a high correlational coefficient with the actual threat landscape.

Cyber Quant Incorporating Threat Intel (Cyber Insights)

Q:What are the key outputs of Cyber Insights?
A: Cyber Insights processes collected threat intelligence in order to output threat landscape trends and patterns. These can be queried on Cyber Insights Analyst and visualized according to selected parameters tailored to an organization's circumstances. Cyber Insights also outputs short-term threat landscape predictions. Cyber Insights outputs can be exported in csv and png. formats.

Q: Can we use Cyber Insights for 2 regions/locations to get a comparison of these?
A: Yes, Cyber Insights can be used to compare threat landscape trends between different regions as well as industries. When selecting threat landscape element parameters, users can also select the depth level they wish to visualize the trends in, enabling a comparison between 2 or more entities in the same depth level. If users wish to compare between entities in different depth levels or threat landscape vectors, they can create two different queries and view them side-by-side on the dashboard.

Q: Can Cyber Insights do forecasts into the future? What is the maximum time period?
A: Cyber Insights' forecasting algorithm can predict threat landscape trends up to one month into the future, provided there is at least 3 months of historical data to base its statistical regression analysis on. When evaluating predicted threat landscape up to one month in advance, Cyber Insight' forecast has a high correlational coefficient with the actual threat landscape.

Q: Can Cyber Insights replace an organization's Threat Intelligence feeds subscription, and or replace the SOC's function to monitor attacks on the organization?
A: Cyber Insights is a strategic intelligence tool, analyzing broad threat landscape trends and looking to impact organizational cybersecurity strategy and business decisions. It is not a tactical intelligence tool and is therefore not meant to replace a SOC's threat intelligence feeds but rather complement them to provide the "larger picture", or patterns behind day-to-day alerts received by the SOC team.