cyber GRX

CyberGRX Risk Assessment Methodology

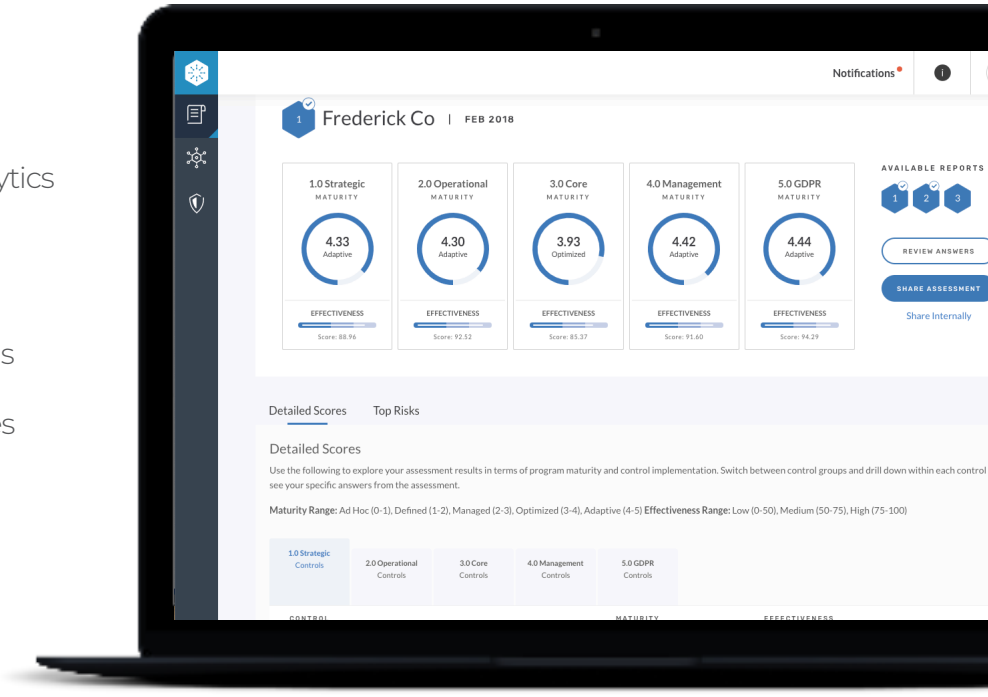
A dynamic assessment approach that supports enterprises and third parties

CyberGRX assessments were designed with practitioners to modernize and streamline redundant and inefficient processes that come with shared and static spreadsheets – for both third parties and their upstream partners. Two of the biggest advantages of the CyberGRX third-party risk assessments: 1. CyberGRX collects data in a structured format and 2. provides that data dynamically via an information exchange. The structured format enables organizations to run analytics across collected data so they can derive actionable insights. And dynamic data ensures ordering customers always have an up-to-date visibility into their ecosystem while enabling third parties to spend less time manually completing disparate spreadsheets and instead move towards completing one assessment that can be shared with many.

CyberGRX assessments are built on NIST 800-53 v4 and ISO 27001 cybersecurity frameworks and map to many other industry standards. CyberGRX assessments are provided in three tiers, covering low, medium, and high risk third parties and include corresponding levels of validation – from self-attestation to on-site evidence review – conducted in collaboration with Deloitte. The assessment features skip-level logic and delegation features, so third parties are only asked relevant questions and can delegate questions to the appropriate departments for greater accuracy. Meanwhile, customers awaiting the completion of a third-party assessment can easily track progress on the CyberGRX dashboard.

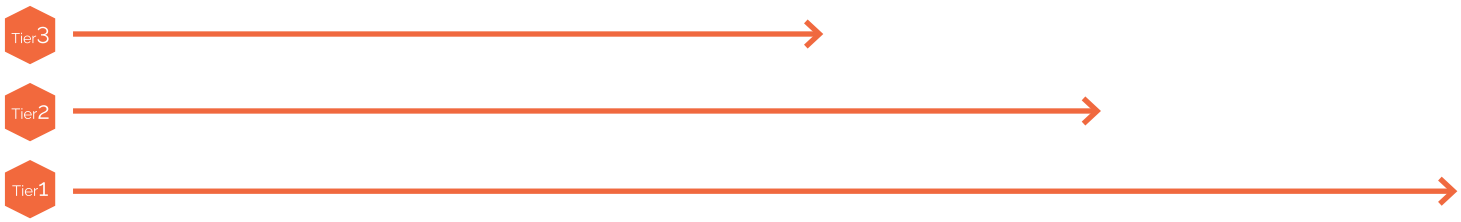
Highlights

- Structured & dynamic data for analytics
- Ongoing & up-to-date visibility via the Exchange
- Tiered assessment & validation levels
- Skip-level logic & delegation features
- Built on NIST, ISO & other common industry frameworks



Assessment Approach

Does your organization employ this control family?	What is the level of control family maturity across people, process, and technology?	Does your organization employ this control?	Does your organization employ the associated sub-controls?	What is the control / sub-control effectiveness across strength, coverage, and timeliness?
28 Control Families (Yes or No)	**196 Measures of Control Maturity (7 Questions per Control Family)** • People: Role, Experience, Training • Process: Policies, Procedures • Technology: Data, Tools	**111 Controls (Yes or No)**	**233 Sub-controls (Yes or No)**	**699 Measures of Control Effectiveness (3 Questions per Control / Sub-Control)** • Strength: The policies, rules, and settings of the control • Coverage: The extent of implementation • Timeliness: The speed or frequency of the control settings
Control Family Existence	**Measures of Maturity**	**Control Existence**	**Sub-Control Existence**	**Measures of Control / Sub-Control Effectiveness**
28 Yes / No Questions	**196 Single Select Questions**	**111 Yes / No Questions**	**233 Yes / No Questions**	**699 Single Select or Multi-Select Questions**



The CyberGRX assessment methodology identifies both inherent and residual risk and uses real-time threat analysis and independent evidence validation to provide customers with a holistic view of third-party cyber risk posture.

Inherent risks are those that exist prior to evaluating the implementation and effectiveness of cybersecurity controls. Inherent risks are often based on the industry most closely related to the party being assessed. Residual risks describe the cyber risks that persist after taking into consideration the controls that an organization implements to address inherent risks. It is important to consider both inherent and residual risk so that organizations know how to tailor their cybersecurity program and how best to monitor and improve its effectiveness.

What A CyberGRX Assessment Includes

CyberGRX assessments apply a dynamic and comprehensive approach to risk assessment analysis, replacing outdated static spreadsheets as well as the need to repetitively complete or request assessments each year. Our assessments integrate advanced analytics, threat intelligence and sophisticated risk models, based on known breach kill chains, with the vendors responses, to provide an in-depth view of how a vendor's security controls will protect against potential threats. The assessments feature five control groups (Strategic, Operations, Core, Management and GDPR), that include controls and sub-controls based on the following frameworks: FFIEC, ISO 27001, NIST 800-53, NIST 800- 171, NY-DFS, PCI DSS, SOC, etc. And because the assessment data lives on the CyberGRX Exchange, third parties only have to complete it once and simply update the information as they implement new security measures or practices.

How Are CyberGRX Assessments Different?

Traditional Approach	CyberGRX Approach
Static: **Provides a point in time view presented in a spreadsheet**	**Dynamic:** **Ongoing view of dynamic data presented via online dashboards**
Honor System: **Relies on the assessees to interpret questions and provide accurate answers**	**Validated:** **CyberGRX assessments include a variety of validation levels that appropriately correspond to risk level and assessment tier**
Compliance based: **Focuses on evaluating the implementation of controls**	**Risk based:** **Evaluate the strength, coverage and timeliness of controls against the nature of the vendor's services, their industry and external threat intelligence**
Customized: **Bespoke and industry assessments are designed to identify gaps, but the resulting insights are often buried in a spreadsheet**	**Comprehensive + Actionable:** **CyberGRX assessments cover 5 broad control groups including 27 control families, 105 controls, and 226 sub-controls and present the data in a structured and actionable format**

Assessment Tiers & Validation Levels

Tier 1

Tier 1 assessments are typically ordered on your riskiest vendors that create significant business exposure from both a high likelihood and high impact perspective.

You may wish to categorize a vendor as high risk if they have access to Personally Identifiable Information (PII) or if they provide mission critical products or services.

Validation
Remote or Onsite

Tier 2

Tier 2 assessments are generally ordered on vendors that pose significant risk, but are not your riskiest. Significant risk may apply to vendors who have access to your internal networks or customer data.

Tier 2 assessments are a great place to start. They provide in depth analysis of vendor controls, while including human in the loop remote validation or rules-based validation.

Validation
Remote or Automated

Tier 3

Tier 3 assessments are ordered on those vendors which pose the lowest risk to your organization.

A vendor may be categorized as low risk if there is no interconnection between their network and yours, or if they have no access to sensitive data.

Validation
Automated

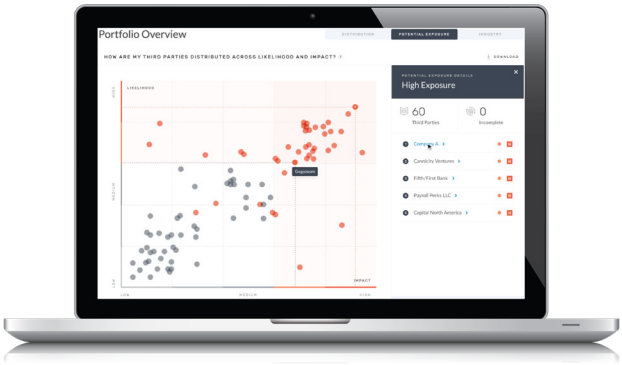
How The CyberGRX Assessment Process Works

The CyberGRX assessment process was designed to help both ordering enterprises and their third parties. Our global risk exchange and dynamic data approach ensures ordering customers have an up to date view of their third-party portfolio and third parties spend less time filling in redundant spreadsheets.

The following workflow summarizes the CyberGRX third-party risk assessment process.

1 Onboard

- Customer adds third parties to the CyberGRX platform
- Customer completes third-party profiles
- Customer receives immediate insights on potential risk and business exposure
- Customer orders appropriate assessments levels on their third parties
- CyberGRX on-boards the third parties

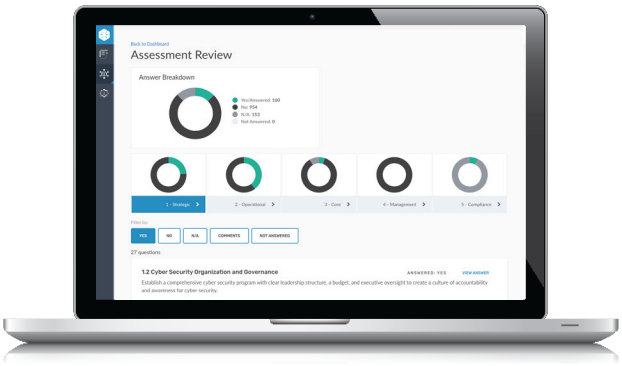


2 Assess

- Third party answers questions related to their business structure and previous cyber incidents
- Third party assigns delegates to help answer cybersecurity control questions
- Third party answers assessment questions, reviews results and submits the completed assessment

3 Validate

- CyberGRX conducts remote validation and works with Deloitte to conduct on-site evidence validation as requested
- CyberGRX finalizes validation analysis and produces a draft assessment



4 Comment

- Third party and CyberGRX review the draft assessment results
- Third party adds comments, if necessary
- Assessment results are finalized

5 Share

- Customers request access to third-party assessment results
- Third party authorizes requests and shares with as many upstream partners as they choose

Read our Pinnacol Assurance case study, to see how CyberGRX transformed their third-party program.

www.cybergrx.com