CyberGRX Risk Assessment Methodology

Assess & Validate Your Third Parties

Data privacy and security are two essential components of a data protection strategy and CyberGRX assessments are the industry's only comprehensive assessment methodology to manage risk across security, privacy, and business continuity. Our assessments come in three tiers and feature skip level logic for easy completion and validation for trusted results. CyberGRX modernizes and streamlines redundant and inefficient processes that come with shared and static spreadsheets.

- An inside out validated approach that dynamically updates as threat levels change or as a vendor updates their security posture
- An enterprise-level assessment that produces standardized and structured data for analysis and benchmarking
- Maps to industry standards and frameworks (NIST –800.53, NIST-CSF, ISO 27001, PCI-DSS, HIPAA, etc.)
- Applies attack scenario modeling and inherent risk analysis against assessment results to create a prioritized control gap analysis

Assessment Tiers & Validation Levels

There are three tiers of CyberGRX assessments, covering low, medium, and high risk third parties. They include corresponding levels of validation – from self-attestation to onsite evidence review conducted in collaboration with Deloitte.

TIER 1

Tier 1 assessments are ordered on third parties that are 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 critical risk if they have access to Personally Identifiable Information (PII) or if they provide mission critical products or services.

TIER 2

Tier 2 assessments are ordered on vendors that pose high risk. This categorization may apply to vendors who have access to your internal networks or customer data.

These are a great place to start as they provide in-depth analysis of vendor controls, while including humans in the loop for remote validation or rules-based validation.

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.

Assessment Methodology

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

Inherent risk describes risk when all cybersecurity controls fail or are missing. It provides a worst-case scenario view and the analysis answers such as:

- What general risk does this third party experience and convey to their customer?
- If a third party has a cyber incident, how bad could it be?

Residual risk describes risk when cybersecurity controls are in place and it's what remains of inherent risk after controls assessment answers tell us what was mitigated. Residual risk analysis answers questions such as:

1. What specific risk does this third-party pose?
2. What types of cyber incidents are likely to affect this third-party?

It's 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.

How Are CyberGRX Assessments Different?

CyberGRX	vs	Traditional Approaches
An online exchange that facilitates data sharing, analysis, and risk prioritization		One-off, redundant requests that require a complete reassessment every year
An inside out, independently validated view of your security posture		Inaccurate outside-in rating on your security posture
Dynamic, cloud-based assessments that you can update anytime		Static spreadsheets that live on a desktop
An assessment that adjusts to your responses and removes irrelevant questions		Multiple irrelevant and redundant questions
Enterprise level assessment that can be shared with multiple customers		Product level assessment tailored to only one customer
Built-in analytics help you identify and address discrepancies in near real-time		Static spreadsheets that only capture what you add

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.

Threat use cases are built on MITRE tactics and techniques that streamline curation, reuse, and modularity, so customers will have better integration with providers who also built upon the framework. This allows CyberGRX to rank susceptibility to specific tactics or techniques a customer may have seen on the news.

The assessments feature five control groups (Strategic, Operations, Core, Management, and Privacy), 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. CyberGRX assessments help customers feel confident in their understanding of how their third parties are managing privacy in respect to the major privacy regulations.

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)	35 measures of control maturity (7 questions per Control Group) **People:** Role, Experience, Training **Process:** Policies, Procedures **Technology:** Data, Tools	105 Controls (Yes or No)	216 Sub-controls (Yes or No)	648 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	35 Single Select Questions	105 Yes / No Questions	216 Yes / No Questions	648 Single Select or Multi-Select Questions

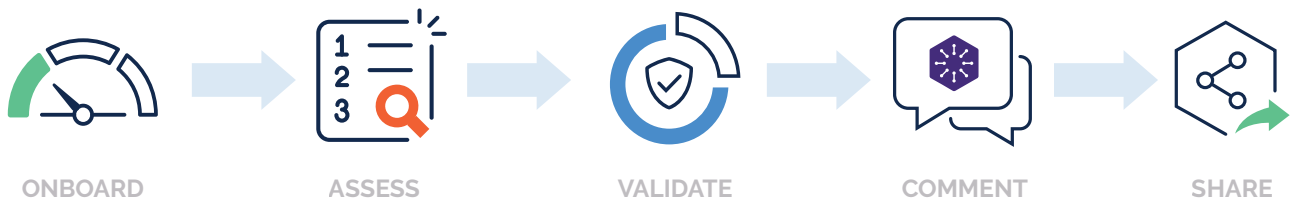
tier 3 →

tier 2 →

tier 1 →

The CyberGRX Assessment Workflow

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



Onboard

- Customer adds third parties to the CyberGRX platform
- Customer completes third-party profiles
- Customer receives immediate Auto Inherent Risk (AIR) Insights™ on potential risk and business exposure
- Customer orders appropriate assessment levels on their third parties
- If the third party is already on the Exchange, they authorize access within a few hours. Otherwise, CyberGRX onboards the third party to the Exchange

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 and submits the completed assessment

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

Comment

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

Share

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

For more information on our assessment methods and the CyberGRX Third-Party Risk Management Platform, visit us online at:

https://www.cybergrx.com/