CyberGRX Risk Assessment Methodology

Assess & Validate Your Third Parties

Developing a data protection strategy is essential to ensure data confidentiality, integrity, and availability at your business and your third parties. CyberGRX's analytical methodology builds threat intelligence and sophisticated risk models from just one validated assessment. With insights on risk across data security and privacy, our assessment features not only in-depth insights on residual risk, but combines attack scenario modeling and the MITRE ATT&CK kill chain to monitor evolving tactics and techniques in the threat landscape. By combining skip-level logic and collaboration for teams, CyberGRX's innovative platform streamlines risk management while leaving spreadsheets in the past.

- An enterprise-level assessment that produces standardized and structured data for analysis and benchmarking
- An inside-out, validated approach that dynamically updates as threat levels change or as a vendor updates their security posture
- Maps to most customer controls as well as industry standards and frameworks (NIST –800.53, NIST-CSF, ISO 27001, PCI-DSS, HIPAA, etc.)
- Applies attack scenario modeling and inherent risk analysis using the MITRE ATT&CK framework 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 recommended for your riskiest third parties who may 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.

Tier 2 assessments are a great place to start as they provide in-depth analysis of vendor controls, as well as 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 questions 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. It's what remains of inherent risk after controls assessment responses tell us what was mitigated. Residual risk analyses answers questions such as:

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

It's important to consider both inherent and residual risk so organizations know how to tailor their cybersecurity program and how best to monitor and improve its effectiveness.

How Are CyberGRX Assessments Different?

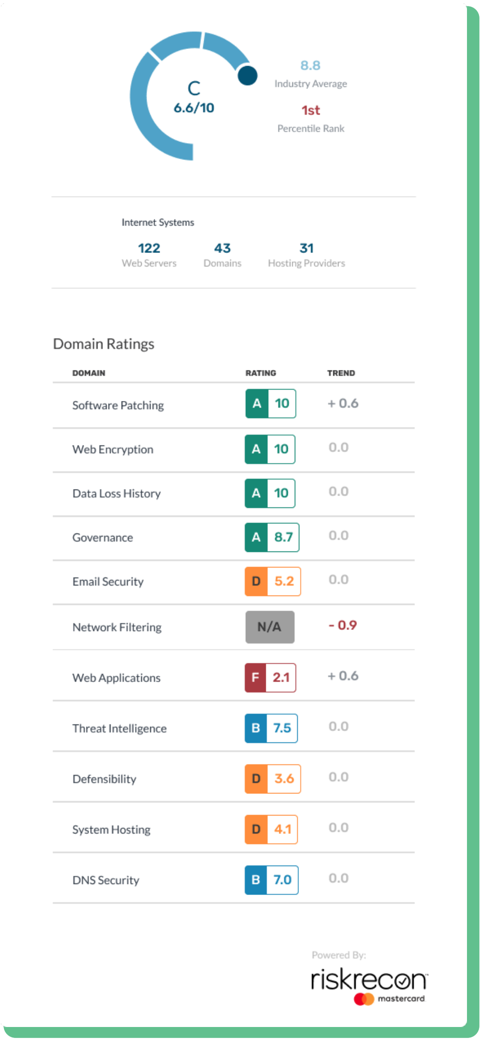
VS

CyberGRX	Traditional Approaches
An online exchange that facilitates data sharing, analysis, and risk prioritization	
Gain immediate visibility into inconsistencies and contradictions within a third-party assessment that highlight potential security gaps through Auto Validation capability	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 vendor responses with advanced analytics, threat intelligence, and sophisticated risk models, based on known breach kill chains, to provide an in-depth view of how a vendor's security controls will protect against potential threats.

CyberGRX uses a data-driven approach that combines third-party cyber risk management expertise with the MITRE ATT&CK® framework. The attack scenario analytics data provides additional context to risk findings so enterprise customers and third parties can better understand gap recommendations in order to improve the overall defensibility of their ecosystem.



Internet Systems

122 Web Servers
43 Domains
31 Hosting Providers

Domain Ratings

DOMAIN	RATING	TREND
Software Patching	A 10	+ 0.6
Web Encryption	A 10	0.0
Data Loss History	A 10	0.0
Governance	A 8.7	0.0
Email Security	D 5.2	0.0
Network Filtering	N/A	- 0.9
Web Applications	F 2.1	+ 0.6
Threat Intelligence	B 7.5	0.0
Defensibility	D 3.6	0.0
System Hosting	D 4.1	0.0
DNS Security	B 7.0	0.0

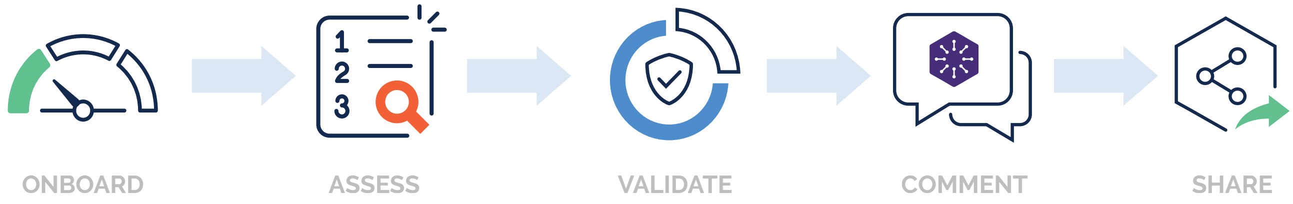
Powered By: riskrecon mastercard

With the addition of RiskRecon performance risk ratings and Recorded Future third-party threat intelligence, CyberGRX users can glean even more insights from their third-party profiles. Using these risk scores, organizations have access to a comprehensive third-party risk profile that arms them with actionable, real-time, risk-reducing insights.

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. 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. The CyberGRX Framework Mapper is a standardized and structured dataset that allows for mapping to most customer controls as well as industry standards and frameworks (NIST –800.53, NIST-CSF, ISO 27001, PCI-DSS, HIPAA, etc.). Our assessments help customers feel confident in their understanding of how their third parties are managing privacy in respect to the major privacy regulations as well as threat profiles based on recent cyber events.

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 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 collaborates with internal experts to ensure cybersecurity controls are answered accurately
- Third party assigns delegates to help answer cybersecurity control questions
- Third party answers assessment questions and submits the completed assessment

Validate

- Auto Validation is applied to assessment enabling customers and third parties immediate visibility into inconsistencies and contradictions into the assessment that highlight potential security gaps in the risk posture
- 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 comments both before and after assessment submission
- 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/