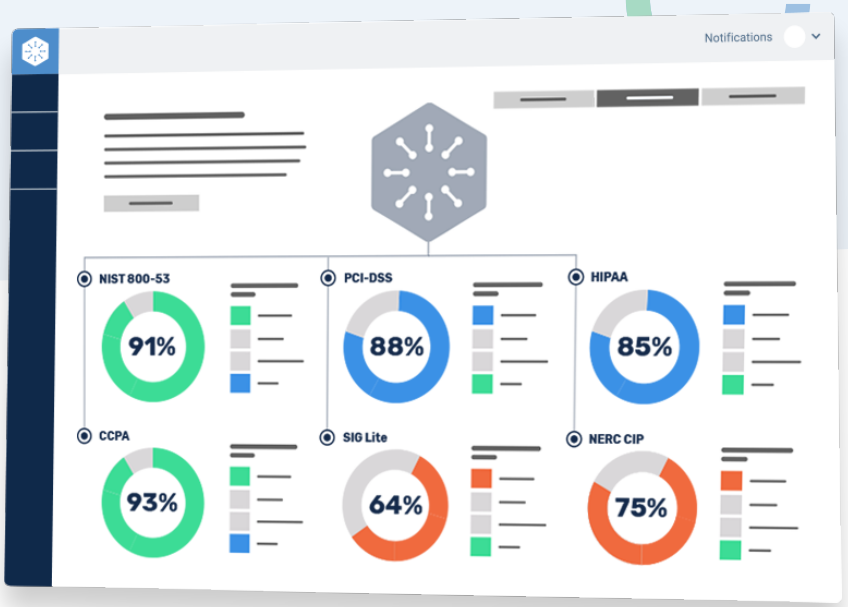
CyberGRX Framework Mapper

Instantly map CyberGRX assessment results against industry or custom frameworks to identify controls coverage and drive remediation

CyberGRX's Framework Mapper allows you to map our award-winning assessment back to industry frameworks to instantly gain visibility into controls coverage, measure data protection policies and standards of third parties, and drive remediation workflows.



Enterprises use a variety of frameworks and compliance regulations to get full visibility and context of third-party risks. Customized assessments used to capture these specific needs result in disparate and unstructured data, making it difficult to consume the resulting data quickly and efficiently.

The CyberGRX Exchange collects assessment data in a structured format that lets you run analytics and derive rapid and actionable insights. This standardized data approach also allows custom output of this assessment using our Framework Mapper. This feature maps assessment results to any industry framework, giving you complete visibility and context of your third-party risk.

Also available within the Framework Mapper tool are threat profiles, which allow both customers and third parties to view coverage of controls that are commonly exploited in cyber attacks. Both common and recent attack profiles are available, and provide visibility to tactics needed to detect, prevent and mitigate common cybersecurity threats.

The ability to map CyberGRX data to other assessments and frameworks means you can move away from custom and redundant approaches, reducing time spent on assessment chasing, and can instead spend your valuable resources on analyzing the data and remediating risks. CyberGRX is the only third-party cyber risk solution on the market that can provide this capability due to our standardized data approach.

Driving risk & cost reduction in managing third-party cyber risk

- Map assessment results to industry frameworks as well as custom frameworks to gain granular visibility into controls coverage.
- Spend time analyzing data and mitigating risk rather than chasing assessments.
- Take advantage of flexible reporting options such as sort/filter by compliance area and domain, controls, benchmark and comparison, etc.
- Benefit from coverage across custom and standard frameworks such as NERC, CMMC, NIST 800/CSF, HIPAA, PCI-DSS, CCPA, GDPR, SIG, and more
- Access to threat profiles to see how third parties rate against commonly exploited controls in attacks

Threat Profiles

Threat profiles in the Framework Mapper are created by examining tactics and techniquesfrom hundreds of use cases, including past attacks, in order to identify the primary controls needed to detect, prevent, and mitigate threats. This data can then be used in ongoing threat monitoring and remediation efforts.

When threat profiles are incorporated into a TPCRM solution, organizations can take advantage of the visibility into how a third party aligns against each identified control. If any controls are missing or absent, the company can follow up with the third party in question to request remediation.

CyberGRX Assessment Methodology

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 with the third party's responses, to provide an in-depth view of how a vendor's security controls will protect against potential threats.

Our assessment approach identifies both inherent and residual risk and uses near real-time threat analysis and independent evidence validation to provide customers with a holistic and validated view of their third-party cyber risk posture. In the absense of an assessment, CyberGRX can also provide predictive results upon immediate ingestion of a third party into our platform, to guide immediate decision-making.

CyberGRX

- An online exchange that facilitates data sharing, analysis, and risk prioritization
- Auto Validation gives immediate visibility into inconsistencies and contradictions within a third-party assessment
- An inside out, independently validated view of your security posture
- Dynamic, cloud-based assessments that you can update anytime
- An assessment that adjusts to your responses and removes irrelevant questions
- Enterprise level assessment that can be shared with multiple customers
- Built-in analytics help you identify and address discrepancies in near real-time

VS

Traditional Approaches

- One-off, redundant requests that require a complete reassessment every year
- Siloed approach that made collaboration between stakeholder departments difficult
- Inaccurate outside-in rating on your security posture
- Disparate spreadsheets that live on a desktop
- Multiple irrelevant and redundant questions
- Product level assessment tailored to only one customer
- Static spreadsheets that only capture what you add

For more information on the CyberGRX Framework Mapping tool please visit our website at:
www.CyberGRX.com