

Reducing Cyber Risk for Organizations Worldwide

The only third-party cyber risk management (TPCRM) solution security professionals need to confidently act on third-party cybersecurity risks

TPCRM is a critical component to any organization's cyber security. Unfortunately, many third-party security programs are plagued with outdated and inefficient processes that drain resources and provide little insight. As third-party related breaches continue to increase, it's time to apply a modern approach to cyber risk management.

The CyberGRX Exchange is a central hub where enterprises and third parties can easily access, order, and share risk data. The Exchange replaces static spreadsheets with dynamic data, so enterprises always have the most current view of third-party risk and can manage it with speed and certainty. CyberGRX gives you a prioritized risk map of your entire vendor population and delivers validated risk assessments on any vendor

Working with industry leaders like Aetna, ADP, Blackstone, Mass Mutual and others, we have the world's largest cyber risk exchange with over 100,000 participants. Because of the dynamic and scalable nature of the Exchange, organizations and third parties work together in a one-to-many fashion to crowdsource data, insights, and remediation strategies. Rich with validated data and analytics, the CyberGRX Exchange is where organizations go to identify, prioritize, monitor, and reduce third-party risk.

Benefits of CyberGRX

- Manage your evolving third-party ecosystem with an ever-growing exchange
- Select from optional additional Client Services offerings that are tailored to help you capture more value from our award-winning platform so you can confidently act on third-party cyber risks
- Increase visibility with Attack Scenario Analytics that uses the MITRE® Framework to apply attack scenario modeling and inherent risk analysis against assessment results to create a prioritized control gap analysis
- Identify trends and create benchmarks by leveraging the structured data on the Exchange
- Be assured that your vendors' security postures are continuously monitored based on the domain cyber hygiene and industry intelligence gleaned from partners such as Recorded Future and RiskRecon
- Strengthen your relationship with your customers and third parties by working together on risk mitigation strategies
- Proactively manage and communicate your mitigation efforts via the Exchange with your upstream partners
- Map to most customer controls as well as industry standards and frameworks via Framework Mapper
- Share trends and insights with your board and other areas of your organization to collaborate and proactively mitigate risk
- Speed up assessment orders and gain visibility into inconsistencies and contradictions in a third-party's assessment with the Auto Validation feature



Identify & Prioritize Your Third Parties

Get rapid and automated insights and instantly create and prioritize a risk mitigation and assessment strategy with CyberGRX's Auto Inherent Risk (AIR) Insights™

- Automate inherent risk insights across your entire vendor portfolio via crowdsourced data from the exchange
- Instantly create and prioritize a risk mitigation and assessment strategy upon ingesting your vendor portfolio
- Be assured that your vendors' security postures are continuously monitored based on domain, cyber hygiene, and industry intelligence
- Review vendor benchmarking across industry, ecosystem, and similar vendors in the exchange

Assess & Validate Your Third Parties

CyberGRX cloud-based assessments are the industry's only comprehensive assessment methodology to manage risk across security, privacy, and business continuity

- Dynamically updating assessments that produce standardized and structured data for analysis and benchmarking, and always show a vendor's most current security posture
- Gain immediate visibility into inconsistencies and contradictions in a third-party's CyberGRX Assessment that highlight potential security gaps in their risk posture with Auto Validation
- Maps to most customer controls as well as industry standards and frameworks (NIST –800.53, NIST-CSF, ISO 27001, PCI-DSS, HIPAA, etc.) via Framework Mapper
- Attack Scenario Analytics uses the MITRE® Framework to apply attack scenario modeling and inherent risk analysis against assessment results to create a prioritized control gap analysis
- Satisfies privacy-related requirements, focusing on the Identification, Governance, Control, Communication, and Protection of data which means comprehensive coverage for increasingly global privacy regulations

Reduce Risk With Validated Data, Analytics, and Benchmarking

CyberGRX integrates threat intelligence with our structured and validated data sets and applies advanced analytics across those data sets to identify insights and help you reduce risk

- Illuminate, remediate, and reduce vendor risk based on automated inherent risk and attack scenario modeling
- Continuously monitor your vendors' security postures based on the domain cyber hygiene and industry intelligence gleaned from partners such as Recorded Future and RiskRecon
- Review a before and after comparison of inherent and residual risk to identify the type of attacks your third parties are susceptible to
- Seamlessly integrate CyberGRX data into existing vendor risk management processes



The CyberGRX Approach to Reducing Risk

Third-party cyber risk management is more than just assessments and security ratings. With proven results, leadership can be confident that the best TPCRM solution is protecting the organization.

The CyberGRX solution integrates advanced analytics, threat intelligence, and sophisticated risk models, based on known breach kill chains, with the vendor's responses. It provides 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 build upon the framework.

Our Framework Mapper feature maps to most customer controls as well as industry standards and frameworks such as NIST -800.53, NIST-CSF, ISO 27001, PCI-DSS, HIPAA, etc. It takes standard data as input and produces custom output across many custom and industry framework controls to quickly and easily provide risk identification, visibility, and reduction.

Reduce risk the CyberGRX way:



Organize

Work with a structured and standardized data set that allows you to run analytics across it and prioritize risk



Benchmarking

Compare individual vendors or entire populations to others on the exchange for benchmarking and risk reducing insights



Strategize

Create a remediation strategy with the most yield leveraging security gap and benchmarking insights



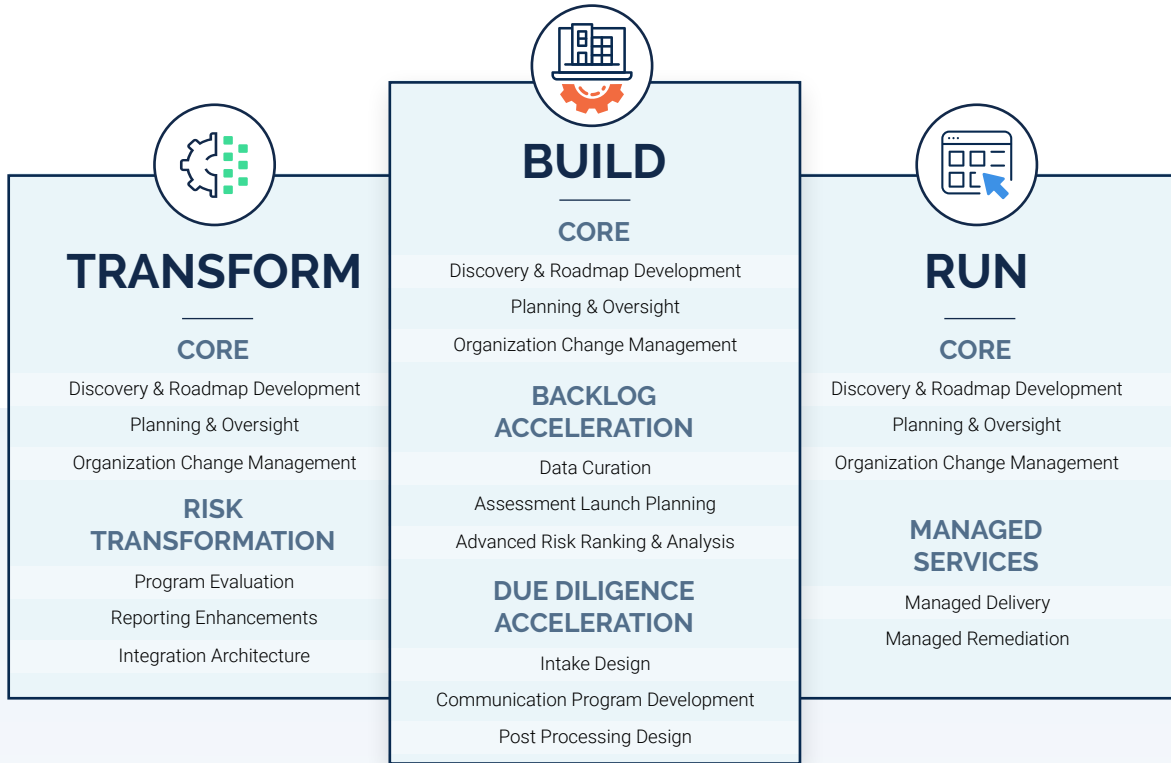
Protect

Feel confident in your understanding of how your third parties are managing privacy in respect to the major privacy regulations

<div style="text-align: center; font-size: 2em; font-weight: bold; margin-bottom: 10px;">CyberGRX</div> <div style="text-align: center; font-size: 1.5em; font-weight: bold; margin-bottom: 10px;">An online exchange that facilitates data sharing, analysis, auto-validating, and risk prioritization using continually updated data</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold; margin-bottom: 10px;">An inside out, independently-validated view of your security posture</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold; margin-bottom: 10px;">Dynamic, cloud-based assessments allowing for team collaboration to ensure the right person within the organization is answering the questions for optimized data accuracy and quality</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold; margin-bottom: 10px;">An assessment that adjusts to your responses and removes irrelevant questions</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold;">An auto-validated assessment that can be shared with multiple customers</div>	VS	<div style="text-align: center; font-size: 2em; font-weight: bold; margin-bottom: 10px;">Traditional Approaches</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold; margin-bottom: 10px;">One-off, redundant requests that require a complete reassessment every year</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold; margin-bottom: 10px;">Inaccurate outside-in rating on your security posture</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold; margin-bottom: 10px;">Static spreadsheets that live on a desktop which can lead to versioning issues</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold; margin-bottom: 10px;">Multiple irrelevant and redundant questions</div> <div style="text-align: center; font-size: 1.2em; font-weight: bold;">Product level assessment tailored to only one customer</div>
---	----	---

CyberGRX Client Service Packages

Our service packages are designed to meet your specific needs and desired outcomes. Our team of third-party cyber risk experts bring years of knowledge and experience to help you determine the right level of engagement and support needs. All centered on the cutting-edge CyberGRX platform, our client services help you take your third-party cyber risk management program to the next level.



PROGRAM: TRANSFORM

Level up the maturity of your third-party cyber risk management program or overcome challenges and roadblocks. With specialized areas of focus on program evaluation, reporting enhancements, and integration architecture, this package helps you overcome third-party cyber risk management program challenges so you're able to provide meaningful and actionable data to your stakeholders, allowing for a truly integrated and collaborative third-party risk management program.

PROGRAM: BUILD

Design and implement a third-party cyber risk management program from the ground up, built to suit your organization's needs. This package focuses on third-party cyber risk management programs that are in an earlier stage. Goals include building program capabilities to enable your organization to manage the risk of new third parties brought into your environment as well as identifying and analyzing a specific scope of third parties to be assessed and developing a strategy to assess and manage risk for that population.

PROGRAM: RUN

Our managed service offerings allow you to fully outsource the third-party risk assessment lifecycle from intake to remediation. As part of this managed service offering, you'll have an embedded delivery resource to assist with third-party assessment completion as well a senior-level consultant who will plan, design, implement, and oversee the delivery of these services.

Visit our website to learn how CyberGRX is a force multiplier that helps you create an efficient, effective, and scalable third-party cyber risk management program