UpGuard™

A Complete Guide to

Third-Party Risk Management

Trusted by hundreds of companies worldwide

PagerDuty NYSE hopin iag ICE TDK

UpGuard

Table of Contents

Introduction iii

Getting Started With Third-Party Risk Management 1

- What is a Third-Party? 2
- What is Third-Party Risk Management? 3
- Third-Party Risk Management vs. Vendor Risk Management 5
- Do you Need a TPRM and a VRM Solution? 6

The Third-Party Risk Management Lifecycle 7

- The Third-Party Risk Management Lifecycle 8
- Integrating a Feedback Loop 12

How to Evaluate Third-Party Risks 15

Common Challenges of Third-Party Risk Management 18

Integrating a TPRM with Your Existing Framework 21

Introduction

If you're currently outsourcing to third-party entities, you're increasing your risk exposure to a data breach. Each of your vendors has some level of access to your internal systems, so if one of them suffers a data breach, they could quickly turn from a trusted partner into a critical attack vector.According to the 2022 Cost of a Data Breach report by IBM and the Ponemon Institute, vulnerabilities in third-party software (one of many third-party risk categories) were the third most expensive data breach attack vector in 2022, resulting in damages of up to USD 4.55 million (an increase of 13% compared to 2021). An effective Third-Party Risk Management Program reduces vendor security risks leading to data breaches, which also reduces the risk of costly damages associated with these events.

https://www.ibm.com/reports/data-breach

UpGuard

Getting Started with Third-Party Risk Management

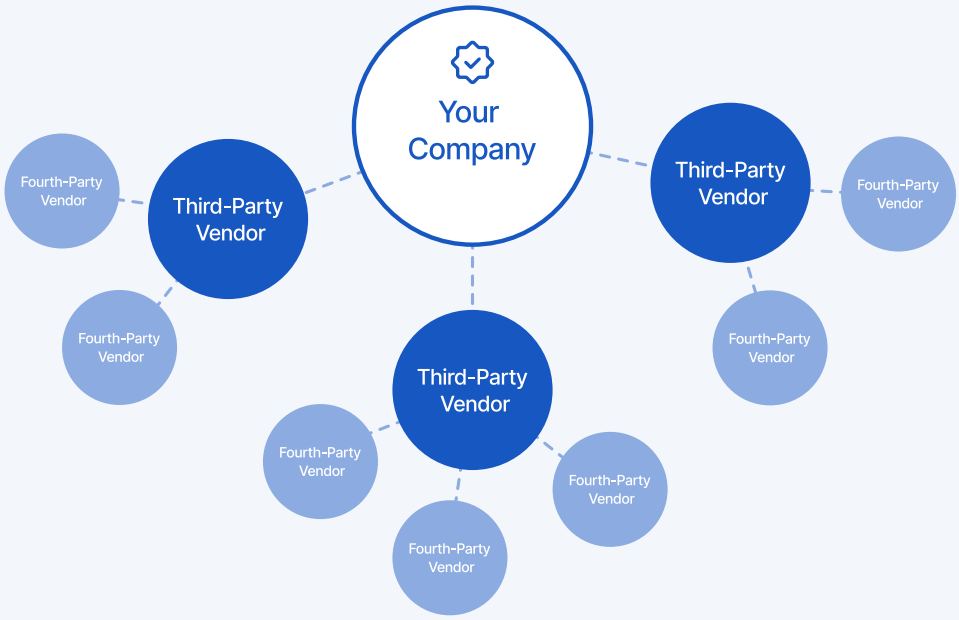
What is a Third-Party?

A third party is any entity that your organization works with. This includes suppliers, manufacturers, service providers, business partners, affiliates, distributors, resellers, agents, and vendors.

Because third-party relationships are vital to business operations, Third-Party Risk Management is an essential component of all Cybersecurity programs.

What's the Difference Between a Third-Party and a Fourth-Party?

A third party is a supplier, vendor, partner, or other entity doing business directly with your organization, whereas a fourth party is the third party of your third party. Fourth parties (or "Nth parties") reflect relationships deeper in the supply chain that are potential avenues to your sensitive resources through your third parties.



What is Third-Party Risk Management?

Third-Party Risk Management (TPRM) is the process of analyzing and minimizing risks associated with outsourcing to third-party entities, such as vendors, service providers, contractors, customers, etc.

Third parties increase the complexity of your information security for several reasons:

1. Third parties aren't typically under your control, nor do you have complete transparency into their security controls. Some vendors have robust security standards and good risk management practices, while others leave much to be desired.
2. Each third party is a potential attack vector for a data breach or cyber attack. A vendor with a security vulnerability could be exploited to gain access to your organization. The more vendors you use, the larger your attack surface and the higher the risk of being impacted by third-party breaches.
3. General data protection and data breach notification laws like GDPR, CCPA, FIPA, PIPEDA, the SHIELD Act, and LGPD are increasing their inclusion of TPRM-related controls and standards, which means there are now financial repercussions for inadequate TPRM efforts.

Insecure third-party vendors are common causes of data breaches. In 2014, Target suffered a data breach after its sensitive network credentials were stolen from an HVAC contractor working at several Target locations. The breach resulted in the theft of 40 million debit and credit card accounts between Nov. 27 and Dec. 15, 2013.

An increasing emphasis on third-party risk management in both regulations and cyber security frameworks is driven by increasing vendor-related security risks. Currently, approximately thirty percent of data breaches are caused by third parties. This concerning statistic will only grow as these attacks evolve in complexity and further outgrow outdated TPRM models.

To sustain businesses in 2023 and beyond, TPRM programs need to adapt to the fast-evolving third-party risk landscape. Organizations that implement such an innovative TPRM model invest, not only in their current state of cyber threat resilience, but also in their future growth. With the impact of third-party data breaches gaining weight in risk analysis calculations, it's the businesses with a proven TPRM program that will win the profitable partnership opportunities of the near future.

88%

88% of organizations have low confidence in the quality of their TPRM process.

30%

30% of data breaches are directly caused by third parties.

60%

60% of organizations will use cybersecurity risk as a significant determinant in conducting business engagements by 2025.

Third-Party Risk Management vs. Vendor Risk Management

TPRM and VRM are often used interchangeably, but there are key differences.

Vendor Risk Management

Vendor Risk Management focuses on mitigating security risks associated with vendors.

Third-Party Risk Management

Third-Party Risk Management extends the scope of risk mitigation beyond vendors to include all third-party entities such as business partners, contractors, customers, service providers, etc. TPRM is an overarching category of third-party risk mitigation that covers VRM and other disciples, including supply chain risk management, compliance risk management, and contract risk management.

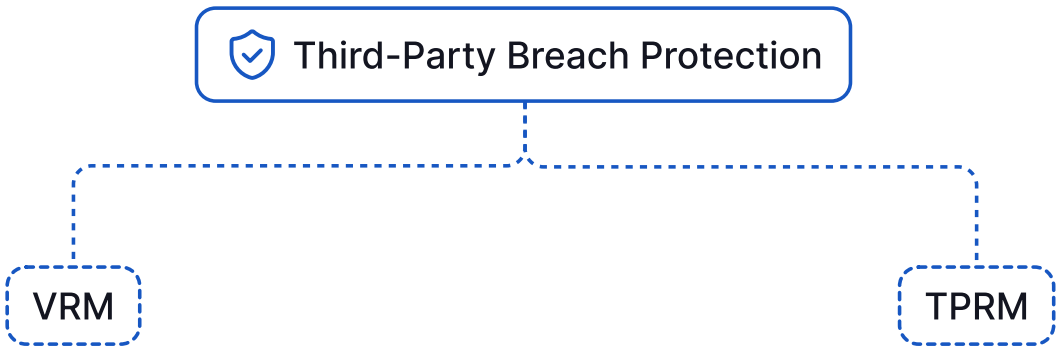
While TPRM could address all third-party risks (similar to a Digital Risk Protection Service), this effort is commonly concerned with third-party security risks.

Do You Need a Third-Party Risk Management and a Vendor Risk Management solution?

A third-party cybersecurity program should include both a TPRM and VRM component since each discipline focuses on a specific scope of risk management.

Vendors, with their ongoing access to sensitive systems, require a unique degree of risk monitoring, both on an attack surface and regulatory compliance levels. Contractors, customers, and other third parties introduce a more nuanced set of security risks that can only be effectively managed with a dedicated risk management program.

By applying tailored risk mitigation efforts across two primary categories of third-party attack vectors - vendors and third-party entities, the combination of a TPRM and VRM program gives organizations the most comprehensive protection against third-party breaches and other forms of cyberattacks involving third parties.



UpGuard

The Third-Party Risk Management Lifecycle

The Third-Party Risk Management Lifecycle

To ensure the ongoing efficacy of third-party risk management efforts, a TPRM strategy must be capable of adapting to the increasing complexity of third-party vendor relationships.

The Changing Roles of Third-Party Vendors

Percentage of legal and compliance leaders agreeing with each statement.

80%

Third-party vendors are performing new technology services.

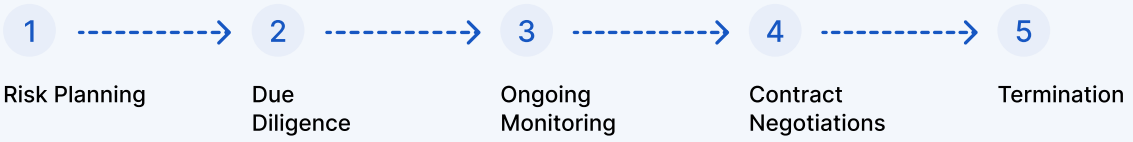
66%

Third-party vendors are increasingly providing services outside of the company's core business model.

Source: 2019 Gartner Third-Party Risk Management Model

TPRM Lifecycle

Ongoing management of evolving third-party security risks is possible with the following 5-stage TPRM lifecycle.



1. Risk Planning

- **Evaluate your third-party risk appetite** - Based on acceptable inherent and residual risks. This risk appetite will likely be modified after onboarding when applicable regulatory and compliance requirements are considered in greater detail. After such considerations, final alignment with your risk threshold could be measured with resultant residual risk ratings.
- **Evaluate and determine how to best tier your vendors** - This is an important step that's often overlooked. Tiering vendors based on the information they will have access to, the product/service they're providing, or their regulatory/ compliance requirements will help you determine the level of risk monitoring and due diligence each vendor requires. Intelligent vendor tiering will also help you track the reassessment (or recertification) schedules of each vendor grouping.
- **Confirm the validity of due diligence processes** - All due diligence risk assessments should be confirmed with a security rating scoring system based on multiple attack vectors.

2. Due Diligence

- **Determine critical due diligence questions** - Multiple data sources should be referenced when designing these questionnaires, including previous quarterly risk reports, internal audit reports, industry standards/regulations, and previously completed risk assessments.
- **Evaluate each vendor's inherent risk score** - Before considering any third-party security controls that will be required in a partnership arrangement, a security risk baseline should be established through a simple risk assessment or questionnaire. This will help you determine the level of controls needed to keep each vendor's risk exposure within your risk appetite limits.
- **Confirm the validity of due diligence processes** - All due diligence risk assessments should be confirmed with a security rating scoring system based on multiple attack vectors.

3. Contract Negotiations

- **Establish security standards in vendor contracts** - This will depend on the jurisdiction you operate in.
- **Consider relevant data breach notification periods** - Depending on your region and the regulations that apply to your organization, you may have minimal third-party vendor breach notification timeframes your vendors should agree to.
- **Complete internal security breach clauses** - Include a contract stipulation to report any minimal internal security incidents not classified as public data breaches (it's better to be overinformed about the security posture of your vendors than underinformed). These events could be communicated in a General Incident Report.
- **Complete ESG clause** - Compliance with specific environmental, social, and governance standards is becoming an increasingly important inclusion in supply chain relationship contracts.

- **Consider adding a 'Right to Audit' clause in vendor contracts** - This will give you the right to review each vendor's internal security processes, audits, self-assessments, and controls.
- **Review stipulated SLAs** - To ensure the standards meet your business and compliance requirements.
- **Seek TPRM platform onboarding approval** - Confirm the vendor's approval of being onboarded onto your company's TPRM platform.
- **Segregate each TPRM project** - Designate an internal primary business owner of each TPRM relationship.

4. Ongoing Monitoring

- **Implement continuous attack surface monitoring** - Implement systems that track the performance and status of all third-party security controls that are in place.
- **Establish internal monitoring triggers** - Monitoring systems triggered during critical security events, such as weakening security postures and deviations from regulatory compliance standards.
- **Implement service level agreements compliance tracking** - Track and assess alignment with stipulated service standards.
- **Follow a reassessment schedule** - performing routine reassessments of all current vendors based on internal policy and regulatory requirements.
- **Account for new risk exposures** - Following strategic direction changes or any changes to digital products and services, security postures should be re-evaluated to detect new risk exposures.

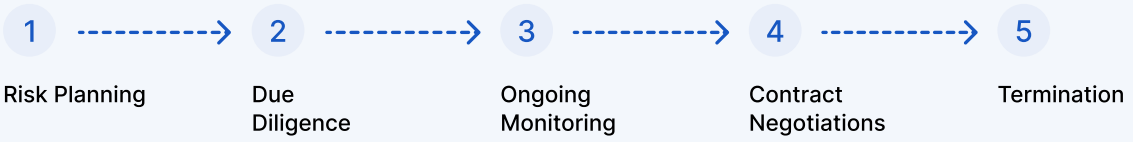
5. Termination

- **Revise user access list after offboarding and contract termination** - Revoke all data access and perform a final review of security policy and regulatory standard compliance.
- **Implement data deletion processes** - In some jurisdictions, data deletion and proof of this action is required. Check your regulation requirements to confirm the need for data deletion and a certificate of deletion confirmation.

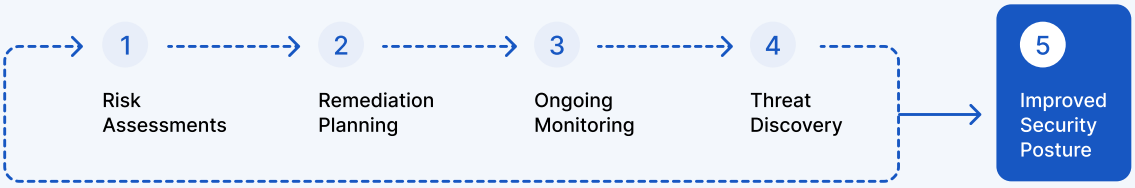
Integrating a Feedback Loop

To further optimize adaptation to changing third-party risks, a feedback loop is added to the TPRM lifecycle to ensure remediation efforts always address emerging risks.

Linear TPRM Lifecycle



TPRM Lifecycle with Feedback Loop



Adding a feedback loop creates an iterative model that can adapt to any changes in risk appetites, security policies, regulatory compliance standards, and business relationships.

The updated TPRM lifecycle model can also consider special third-party risks falling outside of the cybersecurity category, also known as special categories of risk.

Special categories (or non-traditional categories) of risk include entities that have the potential of becoming third-party breach attack vectors despite not commonly being targeted by cybercriminals.

The management of special third-party risks is especially an important capability for financial institutions. Regulators are increasing third-party risk scrutiny in the financial sector, and this trend is likely to continue as digital transformation deepens indirect relationships with sensitive financial data.

Common examples of special third-party risk categories are listed below:

- Insurance agents
- Reinsurers
- Brokers
- Third-party administrators
- Powers of attorney
- Indirect lenders
- Correspondent lenders
- Data marketing firms
- Utilities
- Corporate law firms
- Foreclosure and bankruptcy law firms
- Regulated entities
- Financial market utilities
- Lobbying firms
- Affiliates

Third-Party Risk Management doesn’t have a destination. It's an ongoing process of learning and adjusting to each vendor's emerging security risks.

UpGuard

How to Evaluate Third-Party Risks

How to Evaluate Third-Party Risks

There are various solutions and methods that exist for evaluating third parties. Generally, senior management and the board will decide on the best methods to choose, depending on your industry, number of vendors, and information security policies.

Security Ratings

Security ratings are an increasingly popular part of third-party risk management. They can help with the following:

- Understanding the scope of third-party and fourth-party risks in a supply chain and vendor network.
- Cyber insurance underwriting, pricing, and risk management by allowing insurers to gain visibility into the security program of those they insure to better assess and price their insurance policies.
- Investment in or acquisition of a company by providing organizations with an independent assessment of an investment or M&A target's information security controls.
- Enabling governments to better understand and manage their vendors' cybersecurity performance.

Security Questionnaires

Security questionnaires (or third-party risk assessments) are designed to help you identify potential weaknesses among your third-party vendors, business partners, and service providers that could result in a data breach.

Penetration Testing

Penetration testing (also known as pen testing and ethical hacking) is the practice of testing a computer system, network, or web application's cybersecurity to discover exploitable security vulnerabilities. Pen-testing third-party vendor solutions could uncover overlooked third-party risks.

Virtual and Onsite Evaluations

Virtual and onsite evaluations are typically performed by an outside entity and can include policy and procedure reviews and physical reviews of security controls.

How UpGuard Helps?

UpGuard can help you evaluate third-party risks with:

- An industry-leading questionnaire library based on popular regulations.
- A custom questionnaire builder for highly-targeted risk evaluations.
- A complete third-party risk assessment workflow for seamless risk remediation.
- An industry-leading security rating feature offering instant, accurate insights into vendor security postures.
- A questionnaire risk-mapping feature identifying regulatory compliance gaps.
- A proprietary vendor data leak detection engine reviewed by world-class cybersecurity analysts to remove false positives.

UpGuard

Common Challenges of Third-Party Risk Management

Common Challenges of TPRM

There are several common difficulties most organizations face when implementing and running a third-party risk management program.

Lack of understanding of the need for a TPRM program

Third-party risk management is still a relatively new field of cybersecurity, and as such, many organizations have a limited understanding of how it fits within an existing cybersecurity program. This poor awareness results in an inadequate risk mitigation framework and risk appetite consideration, feeding increasing exposure to third-party security events.

Lack of Speed

It's no secret that getting a vendor to complete a security questionnaire and processing the results can be a lengthy process. A process that is made worse when questionnaires come in the form of dense spreadsheets with no version control, resulting in an error-prone, time-consuming, and impractical process that doesn't scale.

Lack of Depth

Many organizations make the mistake of believing they don't need to monitor low-risk third parties, such as marketing tools or cleaning services. But in a threat landscape that’s quickly evolving towards third-party cyberattacks, all vendors - even the most innocuous - are potential attack vectors, either through direct cyberattack methods, like security vulnerability exploitations, or indirect methods, such as phishing emails purporting to come from trusted vendors.

Lack of Visibility

Security questionnaires alone reveal the effectiveness of a given vendor's security controls for a single point in time. However, IT infrastructures are in constant flux, and the positive results of a given security assessment may not accurately reflect that vendor's security posture a few months into the future. This is why security ratings are usually used alongside traditional risk assessment techniques.

This combination provides third-party risk management teams with objective, verifiable, and always up-to-date information about a vendor's security controls.

Lack of Consistency

Ad-hoc third-party risk management processes mean that not all vendors are monitored, and when they are, they are not held to the same standard as other vendors.

While it's recommended to assess critical vendors more heavily than non-critical vendors, it's still important to assess all vendors against the same standardized checks to ensure nothing falls through the cracks.

Lack of Trackability

Keeping track of which vendors have been sent security questionnaires and completion rates across a network of hundreds or thousands of third parties is a considerable challenge.

Lack of Engagement

Continuously reminding vendors to complete their risk assessments is probably the most frustrating component of third-party risk management, especially when these reminders keep getting lost within ever-expanding inboxes.

UpGuard

Integrating a TPRM with your Existing Cybersecurity Framework

Integrating a TPRM with your Existing Cybersecurity Framework

A common misconception amongst first-time TPRM adopters is that a TPRM program needs to replace an organization's existing cybersecurity framework.

When Implementing a TPRM program, the objective isn't to replace previous cybersecurity investments but instead to augment TPRM with your existing cybersecurity program to broaden its risk management capabilities.

The following 8-step process will help you map your existing risk controls to a TPRM program. This generic process is compatible with most cybersecurity frameworks.

Step 1: Map the lifecycle of all of your most crucial data

An essential prerequisite to implementing a TPRM is identifying all of your critical data, how it’s classified, where it's stored, and its movements across processes. This mapping effort must extend to the third-party attack surface, identifying all of the vendors accessing your crucial data and their level of access.

The flow of your sensitive data through third-party processes, and each vendor’s level of sensitive data access, can be evaluated with risk assessments.

Step 2: Review your Enterprise Risk Management (ERM) Framework

Your ERM framework should be updated to align with the increasing emphasis on third-party risk controls across regulations and compliance standards.

Updating your ERM framework should trigger an update of all your risk registers across each department. Every business unit across most industries utilizes some degree of third-party service, so every business unit should have a risk register.

If you come across any risk registers that have recently been updated, check to make sure their risk data is based on the most updated list of third-party vendors and products in use.

> After updating a risk register, always confirm its alignment with the risk appetite outlined in your ERM framework.

Step 3: Update Your Corporate Risk Appetite Statement

Update your risk appetite statement to address all third-party risks threatening the achievement of business goals and include plans for identifying and managing those risks.

Your updated risk appetite should be defined at an organizational level and feed into every business unit. This will set an objective risk threshold that every business register is measured against, allowing critical third-party risks at a department level to be easily identified.

Step 4: Draft TPRM security policies

Create TPRM policies to align the cybersecurity objectives of your entire organization against processes outlined in the TPRM lifecycle. Besides an overarching TPRM that you include in your risk appetite statement, TPRM policies should be drafted for each business unit in the context of each unit's unique risk profile.

When writing each TPRM policy, it's important to consider your internal third-party risk requirements (as outlined in your ERM framework) and the compliance requirements of any relevant regulatory standards.

Relevant regulatory standards include those that pertain to your industry and the industries of each of your vendors.

A list of popular compliance standards to support your TPRM policy writing efforts:

- Cybersecurity Maturity Model Certification (CMMC)
- European Banking Authority (EBA)
- Cloud Security Alliance (CSA)
- Financial Conduct Authority (FCA)
- General Data Protection Regulation (GDPR)
- Federal Financial Institutions Examination Council (FFIEC)
- ISO 27001
- ISO 27002
- ISO 27018
- ISO 27036-2
- ISO 27701
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- NIST 800-53
- NIST 800-161
- NIST Cybersecurity Framework (CSF)
- Stop Hacks and Improve Electronic Data Security (SHIELD) Act
- SOC 2
- OCC Bulletins
- PCI DSS

Step 5: Select a TPRM framework

Select a TPRM framework that best unifies your TPRM policies, calculated risk appetites, and ERM framework.

Your selected framework should be capable of the following:

- Highlighting the risks within your appetite and those falling outside of the threshold.
- Identifying all of the security controls your third-party vendors are expected to implement

Step 6: Design Third-Party Vendor Onboarding Contracts and Due Diligence Processes

At this point, you'll have enough personalized third-party risk data available to create security contracts for new third-party vendors and establish your due diligence processes. For an outline of the vendor security contract creation process, refer to stage three of the TPRM lifecycle (add page number).

Vendor due diligence processes include the questionnaires and assessments required to accurately describe each vendor's security posture.

> The terms Security Questionnaire and Security Assessment are often used interchangeably because they both refer to the same due diligence processes.

Your choice of questionnaire depends on your unique compliance and cyber threat mitigation requirements outlined in your ERM framework.

Step 7: Identify all of the Regulations that Apply to You and Your Vendors

Identify all of the regulations that apply to you and your third-party vendors. To support this effort, the list below identifies all of the third-party security controls for popular cybersecurity frameworks and regulations.

Payment Card Industry (PCI)

- 8.3
- 9.9.3
- 12.3.9
- 12.3.10
- 12.8
- 12.8.1
- 12.8.2
- 12.8.3
- 12.8.4
- 12.8.5

The Office of the Comptroller of the Currency (OCC)

- OCC Bulletin 2013-29

ISO/IEC 27001

- 15.1
- 15.2

Sarbanes-Oxley Compliance (SOX)

- APO10.01/APO10.02
- APO10.03
- APO10.04

HITRUST CSF

- 5.02 External Parties
- 05.i Identification of Risks Related to External Parties

Step 8: Implement a Vendor Tiering Policy

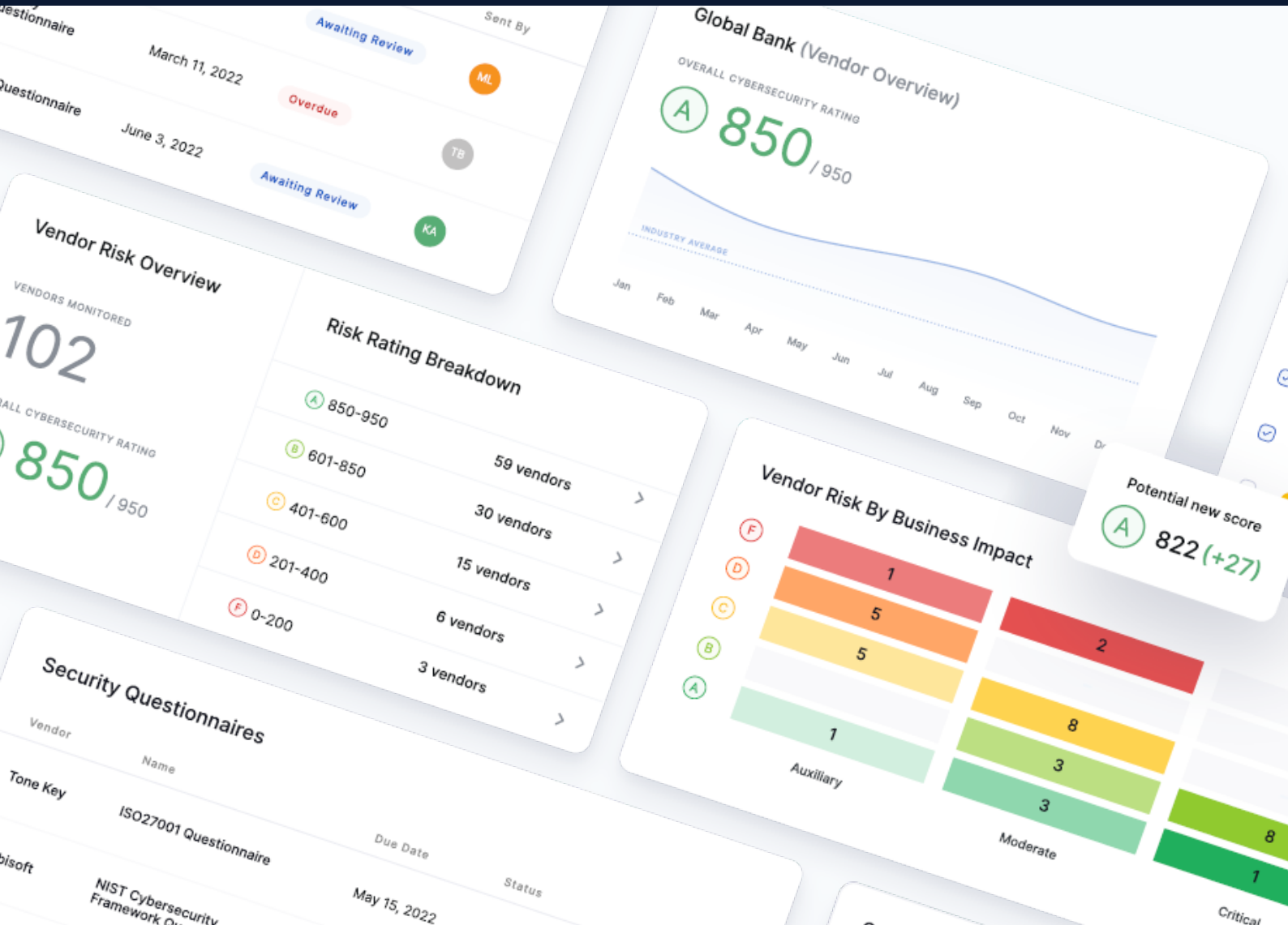
For your TPRM program to be effective, it should prioritize vendors with the highest potential of negatively impacting your security posture. A vendor tiering policy supports this requirement by grouping critical vendors in the same tier, making their cybersecurity impact the primary focus of attack surface monitoring efforts.

UpGuard

Level Up Your Third-Party Risk Management with UpGuard

Prevent third-party breaches, discover potential vendor risks, and track regulatory compliance all from a single award-winning solution.

Free Trial →



UpGuard

We're here to help, shoot us an email at sales@upguard.com

Looking for a better, smarter way to protect your data and prevent breaches?

UpGuard offers a full suite of products for security, risk and vendor management teams.

Free Trial →

Trusted by hundreds of companies worldwide

PagerDuty NYSE hopin iag ICE TDK

www.upguard.com

+1 888-882-3223

650 Castro Street, Suite 120-387, Mountain View CA 94041 United States