Diligent

Technology and Risk Management: A Checklist for Successfully Managing IT Risk and Third-Party Risk

Introduction

As organizations expand their IT footprints, they become more vulnerable to cyberthreats and therefore business risk. Just one well-placed cyberattack can result in data or software damage, breaches of customer information, theft of intellectual property and business interruptions, with the damage rippling out into their supply chain, impacting on compliance with regulators, corporate reputation and revenue streams.

Third parties complicate the risk landscape even further. When organizations trust their facilities, networks and/or data to outside suppliers and partners, they open themselves up to potentially devastating financial, reputational, regulatory, operational and strategic consequences.

What happens if a hacker breaches a SaaS partner's or cloud vendor's systems — and compromises the organization's customer data? Responsibility for risk management falls on the organization. IT and risk teams can never assume that a third party is taking the necessary steps to mitigate threats.

In short, as threats to internal and external IT assets intensify, organizations must stay ahead of these risks, with a strategic plan for risk identification, mitigation, remediation and recovery.

The Challenges of IT and Third-Party Risk

Chief information security officers (CISOs), chief information officers (CIOs), IT leaders, and compliance and risk management teams face a number of challenges in minimizing their organization's IT and third-party risk exposure.

"How can we see out company's risk posture acrosss so many moving parts?"

Risk across internal IT assets and third parties is like a mosaic. Organizations need every tile to grasp the big picture, and they also need to see how the pieces fit together to form a greater whole.

Unfortunately, risk management today too often happens through a siloed approach. Information on IT assets, systems and data comes from disparate business departments and third-party vendors rather than through a centralized platform.

This means that organizations lack the aggregated view they need. Threat indicators and red flags fall through the cracks, and teams are unable to communicate and take action in real time.

"How do we know that the data we're using is up-to-date, reliable and accurate?"

Spreadsheets are ultimately tracking mechanisms, and as such, they fall short of the requirements of today's risk management and compliance teams in many ways.

For starters, spreadsheets aren't equipped to store all types of risk data, such as email conversations. Furthermore, they're difficult to collaborate across and need to be manually updated or re-created to show ongoing progress. They lack security and are easy to manipulate — whether deliberately or accidentally. Finally, spreadsheets — and the risk indicators contained within them — are easy to put into a folder and overlook, making the organization more vulnerable.

"How can we keep up with new risks as they develop?"

The elements in a company's risk profile are always changing, thanks to additions and shifts in internal IT resources, larger and more complex third-party contracts, evolving regulations and more.

A risk program needs to be able to adapt and grow in tandem with these changes, with the ability to add new assets, vendors, contracts and compliance requirements on the fly and streamline complexities along the way. While larger companies with more mature risk management programs are better equipped to tackle these challenges efficiently, siloed systems and static spreadsheets hold organizations of all sizes back in the quest to scale.

“How can we bring all the pieces together and communicate risk in a way that everyone understands?”

IT and risk management leaders presenting to the board, such as CISOs and CIOs, need to deliver an easily digestible summary of risks and opportunities, presented in a way that resonates.

Yet organizations are often held back by poor visibility and poor reporting. For consolidating information, teams often struggle to bring data together across spreadsheets and silos. When it’s time to develop a report, their systems don’t easily allow them to present the information in a manner that’s up-to-date, intuitive and understandable.

“We just don’t have the time or the budget for all of this.”

Collecting data from multiple departments, vendors and outside agencies. Navigating and reconciling multiple spreadsheets. Updating PowerPoints and reports again and again as new information comes in. All this manual labor takes time — and diverts skilled IT and risk management teams away from more strategic, value-added work.

As organizations grapple with these challenges, technology can help. Specifically, solutions exist that offer a centralized and scalable environment, automated workflows and processes, third-party risk management capabilities, and robust visibility and reporting.

The following Risk Management Checklist explores these four areas in greater detail.

A Vicious Circle of Escalating Vulnerabilities

As the growing complexities of IT and third-party risk management strain internal resources, organizations need to find a solution to the problem as soon as possible.

Inadequately staffed and resourced risk management teams put an organization in an even greater state of vulnerability. Vendor service interruptions, ISP failures and data loss may signal greater business interruption, for example, and shared log-in credentials may be red flags that customers’ personally identifiable information is exposed. Organizations miss these indicators at their peril.

Furthermore, an incident like a data breach is not only devastating for an organization’s technical team, but it can also have lasting repercussions for the entire company. GDPR breaches, anonymous data leaks and unaddressed critical incidents not only raise the prospect of significant fines, but they also put a company’s reputation at risk as incidents make headlines. All of the above can have a significant impact on shareholder value.

1. A Centralized and Scalable Environment

What new servers, systems and software have IT teams added to corporate headquarters — and which ones have they retired? Do all these assets comply with the most recent cybersecurity policies, certifications, regulations and requirements?

Looking beyond IT risk management (ITRM), to third parties: Are all vendors up-to-date with their periodic assessments and reviews? Do these assessments reflect the latest compliance requirements? And how compliant and secure are these vendors' cloud providers and other outsourced partners?

To satisfactorily answer all these questions and more, risk management teams must track status, report progress and investigate incidents in a timely fashion. On a strategic level, they must build strategic alignment around the cyber risk and IT risk landscape, making sure to accommodate each department's different goals and priorities.

Unfortunately, too many risk management teams are trying to accomplish all of this across disparate systems, spreadsheets and data sources — putting their departments and organizations at even greater risk.

Enter the centralized, scalable risk management platform. Such a platform gives organizations the integration they need, presenting a single source of truth and enabling real-time communication across departments. The right solution integrates seamlessly with existing processes, systems — both internal and external — and data sources and flexibly adjusts as the organization adds IT assets, third-party vendors, assessment forms, new processes and more.

When evaluating solutions, look for:

□ The ability to merge data from different tools

□ The ability to add, remove and adjust assets as your business grows

□ The ability to customize features as the regulatory landscape evolves

□ Integration with existing systems and processes

□ A unified platform for cross-team collaboration

□ Consistency and visibility across the organization

□ Best-in-class support from leading industry professionals

2. Automated Workflows and Processes

Robust risk management in today's business environment requires both human expertise and technological support — and this is where automation comes in.

Consider all the manual labor involved in IT risk management (ITRM) and third-party risk management (TPRM): cross-referencing vulnerabilities against assets, adding new vendor requests, scheduling vendor assessments and more. Automation supplements human effort by streamlining and strengthening the process. Organizations can deploy preconfigured content with a few clicks and automate critical IT risk & compliance workflows, freeing up their highly skilled staff for more value-added work.

Risk management, compliance and IT staff on the front lines benefit from the significant savings in time and labor. Automation transforms daunting endeavors into tasks that only take minutes.

The organization overall benefits from increased accuracy, security and efficiency. Preconfigured content keeps data standardized and consistent, and automated thresholds, alerts and workflows keep processes moving along, with fewer assessments, investigations and reviews stalled or falling through the cracks.

When evaluating solutions, look for:

□ The ability to deploy preconfigured content in just a few clicks for features like vendor applications and assessments

□ The ability to leverage previous findings, so you're not reinventing the risk management wheel

□ Automation in areas such as issue management, risk reviews and other daily risk management and compliance activities that keep teams diverted from higher-level work

□ Rules-based automation, to ensure that employees or systems don't close issues before all action items are completed

□ Robotic process automation for customized questionnaires and thresholds, as well as triggers and alerts when thresholds are breached

□ Automated, end-to-end risk scoring

□ Seamless integration with threat and vulnerability feeds

□ Features that are intuitive for users across all areas of the business — no specialized training required

□ Best-in-class support from leading industry professionals

3. Third-Party Monitoring and Management

Third parties expand both the scope and complexity of risk management.

Assessments, onboarding and ongoing monitoring can be immensely labor-intensive to manage. The shift to outsourcing and the cloud often brings fourth parties into the mix. And the stakes for getting it right are higher than ever. Any time you trust your facilities, networks and/or data to a third party, you're opening up your organization to potentially devastating financial, reputational, regulatory, operational and strategic consequences.

A third-party risk management (TPRM) solution can help on all fronts. A unified platform empowers organizations to assess, manage and monitor third-party risk with ease, while reducing the risk of error and preventing data duplication. Automation makes TPRM processes, from onboarding to contract management and beyond, more streamlined and secure.

But that's not all a modern technology solution offers for taming the complexities of TPRM. Some solutions integrate information from security and financial intelligence providers, for end-to-end assessment management. Others make it easier to present information to the board, executives and other stakeholders. Visualization dashboards and reports can provide real-time visibility into third-party risk, for example, and advanced analytics can give organizations the ability to quickly identify and prioritize their riskiest third parties. It all adds up to time savings, increased accuracy, a sharper view and more streamlined decision-making.

When evaluating TPRM solutions, look for:

□ A unified platform, with a centralized inventory and data repository

□ A dashboard view, so you can see, at any time, where a vendor is in the onboarding process

□ Pre-built industry standard questionnaires (e.g., SIG Lite and CAIQ-Lite)

□ Bulk import of third-party data

□ Risk-based assessment controls

□ End-to-end third-party assessment management

□ SLA performance monitoring and contract management

□ The ability to collect, measure and monitor data against key performance indicators

□ Integration of third-party intelligence feeds such as credit ratings, IT security risk ratings, media feeds, government watch lists and public filings

□ A platform that integrates with your company's existing systems, including your ERP solution and accounting software

□ Features that enable seamless collaboration for the entire risk management team

□ Ready-to-use visualization dashboards and reports for real-time visibility

□ Best-in-class support from leading industry professionals

4. Powerful Reporting and Deep Visibility

Risk management information only realizes its full value when it's shared — and when the recipients of this information fully understand the data's context, impact and implications.

This kind of reporting and visibility is particularly important for IT and third-party risk management. Leaders, including the board, want to know new vulnerabilities and trends in the cyber landscape, the progress of risk-reduction efforts and how the organization's security posture compares against those of its peers. Being able to provide such visibility is essential to both managing risk across the organization and building trust with the executive team.

Yet preparing risk reports has typically been a convoluted, often ad-hoc process — especially for teams tracking everything in a spreadsheet.

Fortunately, tools are available that help. These ready-to-use visualizations and executive dashboards distill data into an easy-to-understand format, communicating risk to a board that doesn't want complex technical details and enabling low-effort, data-driven decision-making.

When evaluating solutions, look for:

☐ A user-friendly interface that presents data in an easy-to-understand format

☐ A wide range of ready-to-go reporting and visualization options, sharable with anyone who has internet access

☐ Storyboards that let you visually represent data in real time and add context

☐ Integration with threat and vulnerability feeds

☐ A wide range of data connectors and custom APIs for additional (and quick) information retrieval

☐ Connections to risk scores and assessments

☐ In-depth data analytics

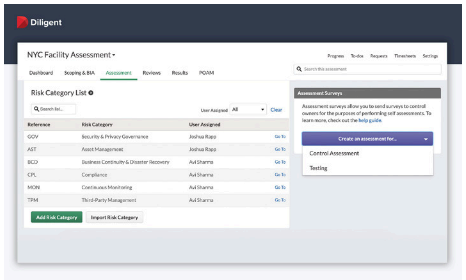
☐ Advanced risk modeling for specific use cases and scenarios

☐ An alert system for elevated risk and action items

☐ Best-in-class support from leading industry professionals

How Diligent Can Help

When it comes to managing risk today, governance technology is the way forward. Organizations should seek a solution that not only covers all aspects of modern risk but is flexible enough to evolve as both the business and the risk landscape around it continue to change and grow.



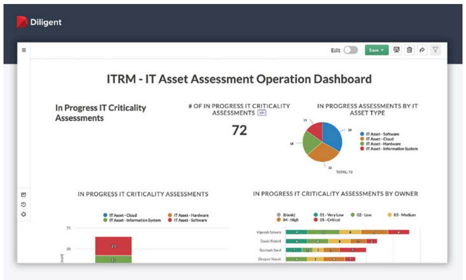
Risk Category List

User Assigned: All

Reference	Risk Category	User Assigned	
GOV	Security & Privacy Governance	Joshua Rapp	Go To
AST	Asset Management	Joshua Rapp	Go To
BCD	Business Continuity & Disaster Recovery	Avi Sharma	Go To
CPL	Compliance	Avi Sharma	Go To
MON	Continuous Monitoring	Avi Sharma	Go To
TPM	Third-Party Management	Avi Sharma	Go To

Assessment Surveys

Assessment surveys allow you to send surveys to control owners for the purposes of performing self assessments. To learn more, check out the help guide.

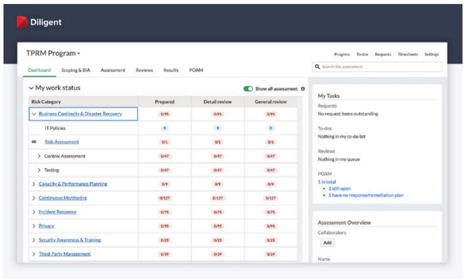

Diligent
Edit
Save
ITRM - IT Asset Assessment Operation Dashboard
In Progress IT Criticality Assessments
# OF IN PROGRESS IT CRITICALITY ASSESSMENTS
72
IN PROGRESS ASSESSMENTS BY IT ASSET TYPE
11
24
15
22
IT Asset - Software
IT Asset - Cloud
IT Asset - Hardware
IT Asset - Information System
TOTAL: 72
IN PROGRESS IT CRITICALITY ASSESSMENTS
IT Asset - Cloud
IT Asset - Information System
IT Asset - Hardware
IT Asset - Software
75
50
Count
IN PROGRESS IT CRITICALITY ASSESSMENTS BY OWNER
(blank)
04 - High
01 - Very Low
05 - Critical
02 - Low
03 - Medium
Vignesh Selvam
David Riddell
Basimah Syed
Deepak Nayak

IT Risk Management (ITRM) from Diligent offers:

☑ Proactive, effective and robust IT risk and compliance management

☑ A centralized and scalable cloud-based platform

☑ A foundational pillar for a proactive, truly integrated governance, risk and compliance (GRC) program — across the entire company



My work status

Risk Category	Prepared	Detail review	General review
Business Continuity & Disaster Recovery	0/95	0/95	0/95
IT Policies	0	0	0
Risk Assessment	0/1	0/1	0/1
Control Assessment	0/47	0/47	0/47
Testing	0/47	0/47	0/47
Capacity & Performance Planning	0/9	0/9	0/9
Continuous Monitoring	0/127	0/127	0/127
Incident Response	0/75	0/75	0/75
Privacy	0/95	0/95	0/95
Security Awareness & Training	0/25	0/25	0/25
Third-Party Management	0/39	0/39	0/39

My Tasks

Requests
No request items outstanding

To-dos
Nothing in my to-do list

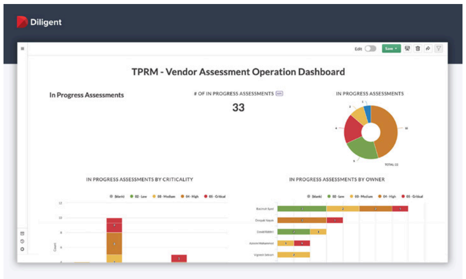
Reviews
Nothing in my queue

POAM
1 in total
- 1 still open
- 1 have no response/remediation plan

Assessment Overview

Collaborators

Name



Third-Party Risk Management (TPRM) from Diligent empowers companies to:

☑ Simplify, manage and scale an existing third-party risk-management program

☑ Establish a solid foundation to create and grow a third-party risk program — whatever the organization's size

☑ Accommodate change and third-party program maturation over time as the business, regulatory and risk landscape evolves

To learn more about how Diligent can enhance your IT Risk Management and Third-Party Risk Management programs, schedule a meeting today.

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS company, serving 1 million users from over 25,000 customers around the world. Our innovative technology gives leaders a connected view of governance, risk, compliance and ESG across their organizations, sparking the insights they need to make better decisions and lead with purpose. Learn more at diligent.com.

For more information or to request a demo:

Email: **info@dligent.com** • Visit: **diligent.com**