A buyer's guide to IT risk management (ITRM) software

Evaluating solutions based on functionality, security, compliance & cost



Diligent

01

Your IT risk management program is only as strong as your weakest asset

Today's organizations face a rapidly evolving risk management landscape, and their IT and information security teams must ensure compliance with ever-changing frameworks, standards and regulations in order to obtain the important security certifications they need to do business.

With just one incident, data can be compromised, software damaged, intellectual property stolen and business interrupted. The repercussions can have a ripple effect across their regulatory compliance, corporate reputation and revenue streams.

Increasing cyber attacks complicate the risk landscape even further as companies shift to outsourcing and the cloud. That's why effective IT risk management (ITRM) programs are intrinsic to success and to growth.

To illustrate this urgent problem, consider the average cost of a data breach is $4.35 million USD and the difference in the average cost of a data breach at organizations without security automation deployed vs. organizations with automation fully deployed is $3.05 million USD[2].

A complicated — and constantly changing — risk and compliance landscape

Information on IT assets, systems and data comes in constantly from multiple departments, vendors and outside agencies, like the individual tiles of a mosaic. To see the full picture, organizations need to consolidate, reconcile and analyze this data.

But this task too often happens through a siloed approach, with teams struggling to bring data together across spreadsheets, systems and reports — only to update it again and again as new information comes in.

[1] https://www.diligent.com/insights/white-paper/third-party-risk-management-essentials/, Opus & Ponemon Institute, 2018, Results of 2018 Third-Party Data Risk Study

[2] https://www.ibm.com/reports/data-breach, Cost of a data breach report 2022, IBM

02

Key challenges: The mosaic of IT risk

With risk today, organizations need to see each individual tile, but also how the pieces fit together to form a greater whole. Without such an aggregated approach, red flags and necessary actions can fall through the cracks. This puts organizations behind the curve for the five phases of management.



Low-value resources for time-consuming tasks

Consider, for instance, the time and effort involved in assessing and monitoring IT risk and regulatory compliance.

Inadequately staffed and resourced risk management teams put an organization in an even greater state of vulnerability. Moreover, all of this time-consuming labor diverts skilled IT and risk management teams away from more strategic, value-added work.

Poorly designed systems for reporting and visibility

Too many tools fall short of today's risk management and compliance challenges. Take the common, ubiquitous spreadsheet, for example.

Spreadsheets are not designed to store many types of risk data, such as email conversations. They're difficult to collaborate across. They need to be manually updated or re-created to show ongoing progress — which often creates a version-control nightmare. At the same time, spreadsheets are also easy to manipulate, compromising data security and the integrity of your operations.

Finally, when it's time to develop a report, tools like spreadsheets aren't user-friendly for the person preparing the information or the one receiving it. They're just not designed to present data in a manner that's current, intuitive and easy to understand.

03

Key considerations when using technology for ITRM

Technology can help — especially solutions with a centralized and scalable environment, automated workflows and processes, and robust visibility and reporting. As an alternative to spreadsheets and manual processes, such tools enable organizations to identify, monitor and mitigate risks more swiftly and securely, share information and adapt to evolving threats.

But not all ITRM solutions are created equal. There are four critical areas to consider:



Functionality



Security



Compliance



Cost

If you're ready to take the next step in ITRM, read on. You'll find the questions to ask a potential vendor in these four areas — and the answers to seek.

04

Functionality

IT Risk teams don't have time for data that's cumbersome to store and time-consuming to access, or disparate systems that result in poor collaboration and competing versions of the truth.

Any technology solution you adopt needs to be a worthy alternative to the spreadsheets, slide decks and manual processes that fall short of today's risk management and compliance responsibilities.

This is where functionality comes in. Here are the questions to ask.

Functionality Q&A

Does the solution bring all the pieces together?

Organization-wide consistency and visibility are key to continuous risk management and remediation. With a unified platform, preconfigured content for applications and forms will help keep your data standardized and consistent, as will coordinated assessments. Meanwhile, system-generated alerts and preparer/approver workflows keep risk reviews moving — and prevent important details from falling through the cracks.

Does the solution "play well with others"?

You'll want a solution that integrates with your existing systems and processes, with the ability to merge data from different tools.

Does the solution save time and streamline processes?

Look for features like built-in risk scores and integration with independent security ratings, so the solution gives you the ability to quickly and efficiently assess, monitor and mitigate both IT risks and third-party risks. Also look for automation and centralized tracking for manually intensive tasks.

How will the solution support data-driven decisions?

Don't let poor visibility and reporting hold you back. Any solution will need to enable you to present your findings quickly and clearly, using the most comprehensive, current data. Look for features like risk matrices and easily digestible summaries of risks and opportunities.

05

Security

In today's hyper-connected world, just one breach or lax security practice can put your entire enterprise at risk — and vendors are often the weakest link. In fact, a PwC study estimated that nearly two out of three cyberattacks could be traced either directly or indirectly to third parties.[3]

The responsibility for risk management falls on your organization; you can never assume a third party is taking the necessary steps to mitigate threats. Therefore, it's even more critical that any ITRM enables you to select compliant and viable third-party vendors.

The right software can help quickly and efficiently assess, monitor and mitigate IT risk, including that of third parties, while staying compliant with the latest regulations. You can then share a concise summary with senior management, the risk committee and the board.

Security Q&A

What about risk prioritization?

Advanced analytics can help you quickly identify and prioritize your riskiest third parties. Some solutions also prioritize risks across vendors in an easy-to-use matrix.

Does the solution provide visibility into the overall cyber risk and IT risk landscape?

Look for user-friendly visualizations of everything from risk prioritization to vendor status, plus dashboards and reports that support strategic alignment and accommodate each department's goals and priorities.

[3] From https://www.diligent.com/insights/white-paper/third-party-risk-management-essentials/ PwC, 2018, The Global State of Information Security Survey

06

Compliance

Regulatory breaches also put a company at risk, incurring not only fines but reputational damage that can have a significant impact on shareholder value.

For compliance purposes, the umbrella of what constitutes a "third party" is vast and ever-expanding: subsidiaries, franchises, vendors, consultants, even charities to which you donate time and money. Meanwhile, the regulations these entities must comply with, from GDPR to new rules by the SEC, are complex and ever-evolving. Failing to comply with these regulations or to obtain the necessary security certifications means businesses could not only face stiff penalties but also miss out on big opportunities.

Compliance Q&A

What are the solution's capabilities for data collection and sharing?

Data collection for compliance operations involves a plethora of data sources and systems. The same complexities apply to the information that goes out for reporting — and this makes information sharing and integration a top priority.

Does the solution play well with all the risk frameworks relevant to your company and industry, such as NIST, ISO, PCI DSS and HIPAA? Will it allow organizations access to sensitive company data as needed — promptly, accurately and securely?

Is the solution customizable?

Especially in the area of IT compliance, every organization has its own processes, procedures and workflows. You'll need a solution that works with yours and that you can easily adapt as the regulatory landscape evolves.

Does the solution leverage automation and other time-saving features?

Tedious daily tasks bog down compliance and risk teams and divert them from higher-level work, so look for features that will save them time and save your organization money. This includes automation in areas such as issue management, risk reviews and pre-built questionnaires for industry standards such as SIG Lite and CAIQ-Lite.

How does the solution track and document progress?

Any solution should make it easier for you to manage IT compliance across your operations and demonstrate to regulators and auditors that you're doing so. Look for features like centralized repositories for surveys and risk assessments, as well as comprehensive audit trails.

07

Cost

You know the business damage that results from improperly managing IT assets and data across your extended enterprise. According to IBM, the average cost of a data breach in the United States is $4.35 million.[4]

Breaches and unplanned maintenance can incur fines and business interruptions, while poorly managed activities like contracts increase vulnerabilities and put revenue at risk.

But your organization's resources may already be stretched to capacity, and there may be uncertainty around implementation, maintenance and the true cost of ownership.

Don't let "we just don't have the time or the budget for all of this" be the enemy of effective, technology-enabled ITRM. Choose a solution that assuages fears about adoption, upkeep and scalability. Most importantly, choose a solution that will demonstrate its ROI, with a proven ability to save employees time and protect your organization against costly data breaches, penalties and reputational damage.

Cost Q&A

How will the solution save employees time?

Automation is a must-have for risk and compliance management, turning daunting manual endeavors into tasks that take only minutes while strengthening accuracy and security. Look for automation capabilities in critical workflows like risk mitigation, scheduling, follow-ups and report generation. Also look for preconfigured content that employees can deploy with just a few clicks.

How easy will the solution be to adopt and use?

Cumbersome, user-unfriendly technology can crush morale. Yet effective tools have the power to improve it, resulting in greater productivity, increased job satisfaction and less turnover. Seek out a solution that's intuitive for users across all areas of the business, requires no specialized training, and offers best-in-class support from industry professionals.

Will the solution grow with your organization?

The right solution will need to not only integrate seamlessly with the processes, systems and data sources you have in place today, but also accommodate your needs into the future. You'll need the ability to easily add IT assets, third-party vendors, assessment forms and new processes, plus the ability to remove and adjust these assets as your business grows.

[4] https://www.ibm.com/reports/data-breach

08

Tips for ITRM software implementation success

As you are assigning risk ratings to your vendors, do not forget to take into account the regulatory requirements for the jurisdictions where you operate. Also, keep in mind, under certain circumstances, your third parties may be outsourcing to fourth and even fifth parties. Other tips include:

- ☐ Get stakeholder buy-in early
- ☐ Create a roadmap based on stakeholder input, and review it
- ☐ Support this roadmap with Specific, Measurable, Achievable, Realistic and Time-bound (SMART) goals
- ☐ Share your plans and progress
- ☐ Use feedback for continuous improvement
- ☐ Keep learning to become an ITRM expert

Diligent ITRM solution

With a centralized and scalable platform, data analytics, automation and real-time reporting and dashboards, the Diligent ITRM solution delivers the visibility, coordination and collaboration risk management, and compliance teams need to manage threats across internal assets and third parties.

With the Diligent IT risk management solution, organizations can:

- Gain a centralized view of complex, multi-stakeholder tasks
- Align controls to numerous different frameworks, including SOC2, ISO 27001 and NIST
- Replace repetitive, manual efforts with automated workflows and data analytics
- Automate risk scoring from end to end, with built-in risk scores and integration with independent security ratings
- Manage your IT compliance program in a FedRAMP and DoD IL5 secured environment
- Save even more time with preconfigured content employees can deploy with just a few clicks
- Demonstrate a robust and continuously monitored compliance posture against key global IT and InfoSec standards
- Access ready-to-use dashboards that summarize your security certifications to reassure the board and the C-suite

Take the next step in your IT risk management program with Diligent.

Request a demo today

About Diligent

Diligent is the global leader in modern governance, providing SaaS solutions across governance, risk, compliance, audit and ESG. Empowering more than 1 million users and 700,000 board members and leaders with a holistic view of their organization's GRC practices so they can make better decisions, faster. No matter the challenge. Learn more at diligent.com.

For more information or to request a demo:

info@diligent.com | diligent.com

© 2023 Diligent Corporation. "Diligent" is a trademark of Diligent Corporation, registered in the US Patent and Trademark Office. "Diligent Boards" and the Diligent logo are trademarks of Diligent Corporation. All third-party trademarks are the property of their respective owners. All rights reserved.