SPONSORED BY

AUDITBOARD

IT Risk & Compliance Platforms: A Buyer's Guide

SC MEDIA CRA | Business Intelligence

ebook
An SC Media publication

How to Choose and Implement an IT Risk and Compliance Platform

Purpose-built IT risk and compliance management software can make your organization more secure and better equipped to respond to new threats and regulatory changes. ***Paul Wagenseil*** *outlines how an ITRC platform works and the key steps to take when choosing and deploying one.*

OUR EXPERTS:

Mary Tarchinski-Krzoska
Market Advisor, Risk and Compliance, AuditBoard

Daniil Karp
Director of Product Marketing, AuditBoard

Dr. Jonathan Creekmore
VP, Information Security Manager, Pacific Western Bank

Chris Patteson
CTO/CISO, The FRONTDoor Collective

Fred Rica
Partner at BPM

Marvin Smith
Founder, NxusCloud

Bryan Willett
CISO, Lexmark International

Organizations face multiple challenges when it comes to their information technology risk and compliance (ITRC) programs.

It’s difficult keeping up with changes to requirements and regulations. Assessments are often rushed and lack the proper thoroughness. Compliance, audit and risk teams aren’t seamlessly communicating due to operational silos that lead to decentralized data and disaggregated reporting, making data-driven decisions impossible.

Risk and compliance programs are usually implemented manually, using annual or twice-yearly company-wide internal risk assessments, evaluations of third-party vendors and, sometimes, external audits. Staffers and vendors must fill out long questionnaires that are then processed and analyzed by risk and compliance teams. These practices may work for smaller organizations, but are too burdensome for larger enterprises with thousands of employees as well as assets and dozens of third-party vendors.

"Instead of understanding why you need to be compliant, you're just going off and checking boxes," says Marvin Smith, Founder at NxusCloud, a New York managed service provider.

In a February 2023 AuditBoard survey of 1,000 compliance, audit and risk management professionals, 23% said their top compliance challenges were "business and technical transformation" while 22% cited "talent management/strained resources." Fifteen percent identified "rapidly changing requirements" and another 12% cited "regulatory expansion." Amid these challenges, two-thirds of respondents said continuous GRC monitoring helps compliance teams be more efficient and proactive.

One solution to these overlapping challenges is an ITRC management platform that can automatically implement framework changes, provide visibility for all stakeholders and, best of all, enable continuous, up-to-date monitoring of your IT risk and compliance posture.

"It is purpose-built software that helps you manage your entire IT risk and compliance program," says Mary Tarchinski-Krzoska, Market Advisor, Risk and Compliance at AuditBoard, which provides such a platform "through incorporating automation throughout the full lifecycle of your program, not just around evidence collection."

IT Risk and Compliance Defined

IT risk and compliance is also known as IT governance, risk (or risk management) and compliance, which is itself a subset of the greater enterprise governance, risk and compliance (GRC) structure.

Any business or organization has known risks that can be managed, enumerated and quantified according to their likelihood and potential impact. For example, ransomware attacks are growing in frequency and severity with the potential to be devastating, making it a high priority for organizations to mitigate that risk by taking steps to lessen the likelihood and impact of a successful attack.

> ***"It is purpose-built software that helps you manage your entire IT risk and compliance program through incorporating automation throughout the full lifecycle of your program."***
>
> — Mary Tarchinski-Krzoska | *Market Advisor, Risk and Compliance, AuditBoard*

"[Risk is] anything that has an impact at some level of monetary loss at some level of likelihood," says Chris Patteson, CTO and CISO of The FRONTDoor Collective, a Dallas-based logistics firm. "Whether it's IT risk, whether it's company risk from a financial standpoint, the human element, all those things, there's usually a monetary loss at some low probability."

Against this backdrop, businesses in most developed countries must follow government regulations such as the U.S. Sarbanes-Oxley (SOX) Act and the European General Data Protection Regulation (GDPR), as well as business standards such as the Payment Card Industry Data Security Standard (PCI DSS). Additionally, most organizations comply with additional regulations such as NIST and ISO to remain competitive, which introduces additional complexity.

Compliance is making sure your organization follows all these rules properly, but it can also refer to a greater framework that ensures operational awareness of security and regulations.

Governance within the context of a private organization is the practice of establishing and enforcing a set of internal policies, rules and guidelines that affect the organization and its employees, managers, directors and shareholders.

Understanding GRC Processes

How well risk management, compliance and governance are handled in an organization can be measured by an internal self-assessment, but an external audit is seen as more reliable.

Governance, risk management and compliance can be handled individually by different teams who have little to do with each other. But over the past 15 years, many organizations have consolidated them into larger GRC programs for the sake of efficiency and transparency.

> *"When I think of IT Risk and Compliance, it really is that process of understanding the risks that are in your environment, but also understanding what the compliance regulatory space looks like."*
>
> — Bryan Willett | *CISO, Lexmark International*

Several frameworks have been developed to assist GRC programs. Those that apply to IT include the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), the related NIST 800-53 and the International Organization for Standardization (ISO) 27001.

Finally, controls are policies or procedures put in place within an organization to mitigate risk, ensure compliance, and carry out governance activities. A password-complexity requirement for all employees is an example of a simple control.

ITRC, or IT GRC, concerns itself chiefly with the information technology aspects of GRC and less with the financial aspects.

"ITRC is more focused on taking a risk-based approach to your compliance program. You not only manage compliance with specific frameworks, you focus on the management of your IT assets and investments in your tech stack, as well as managing the risks associated with those," says Daniil Karp, Director of Product Marketing at AuditBoard.

ITRC does not stand apart from a wider organizational GRC program. Instead, it's part and parcel of a greater whole.

"It's almost impossible to separate [IT and GRC] because everything we do, all our business processes are dependent on IT," says Fred Rica, Partner at California-based accounting firm BPM. "Mature organizations think about it that way. Immature organizations bifurcate the two and that gap can be problematic because the IT controls we might be putting in place, while good, might not actually match up very well to the business risks that we're actually trying to mitigate."

What ITRC Software Platforms Can Do for You

An IT risk and compliance management platform that automates many GRC processes, integrates different teams and enables continuous monitoring and internal auditing may be the solution to bridging the gap between IT and GRC.

If an organization uses a point system outside of an overall GRC, it might have different tools to help manage different parts of its program, Tarchinski-Krzoska says. With AuditBoard, knowing that one's IT risk and compliance solution is part of the overall GRC is reassuring because organizations now have a single source of truth for their IT risk and compliance that can be integrated across all the different areas that fall under GRC.

Continuous automated monitoring enables your organization to recognize and remediate risks and threats more quickly. Continuous automated assessment relieves the workforce from having to fill out questionnaires every six to 12 months. Risk-based decisions are informed by real-time data, not outdated information.

An ITRC management platform also empowers otherwise siloed teams to work together with access to the same data on a shared dashboard, a crucial advantage when different groups are striving toward a common goal.

"Creating that single-pane-of-glass interface is definitely important," says Dr. Jonathan Creekmore, VP and Information Security Manager at Pacific Western Bank. "It can be an automated enabler. I hate to use this word in a civilian context, but it's a combat multiplier, if you will, for awareness and education and training."

When you're buying an IT Risk and Compliance solution, remember that it should not just be a point solution. Instead, the core priority is to have access to a platform that ties in with your audit and risk teams, because there's so much collaboration and cross-functional work that needs to happen for a risk and compliance program to be executed with those teams, Karp says.

The fact that an automated ITRC platform will keep your company updated with regulatory and framework changes in real time is equally important.

"Within the last two years alone, PCI has been updated; ISO 27001, 27002, NIST has been updated, along with [the U.S. Department of Defense's] CMMC, et cetera," says Tarchinski-Krzoska. "For all of those changes, you have to adopt them, understand what they are, and bring them into your environment. It takes a lot of time to get up to speed, perform gap assessments and work around it. Our product is purpose-built to help you manage these challenges."

ITRC Platform Challenges

The aforementioned benefits don't mean there aren't a few potential challenges associated with using an ITRC platform. For starters, an ITRC platform isn't a set-it-and-forget-it solution. While it will make you more compliant and result in less risk, there will likely be some initial investment to lay the groundwork for it.

"[ITRC] requires a fair amount of care and feeding in order to make that system work and be effective. And if you don't care for and feed it regularly, it's quickly going to become garbage," says Willett. "You've got to have the people on it and the process around it in order to make that a valuable tool."

Another potential pitfall is forgetting that all automated processes, even those handling GRC, are fallible and should be closely supervised.

"As you entrust more of these things to machines and those capabilities to these platforms, you need to understand the variables and inputs and make sure you're not getting false positives," says Patteson. "And that also needs to be audited as part of compliance."

Stand-Alone ITRC, or GRC Within IT Service Management?

Many IT service-management tools (ITSM) offer GRC modules that can handle at least basic IT risk and compliance functions. Buying such modules may appeal to organizations that are already using an ITSM and want convenience that's not provided by a stand-alone ITRC solution.

"Now you're just a one-stop shop; everything's already integrated," says Rica. "And that's the big advantage."

However, most of the experts we spoke to advised against GRC within ITSM.

"A management service," says Smith, "[is] not going to be on top of all the minute changes within the industry, because the industry itself is big and a lot of micro-subsections are constantly changing."

To Mary Tarchinski-Krzoska at AuditBoard, an ITSM tool is not able to deliver the same quality of results that a dedicated connected risk platform can.

"The total cost of ownership is very high," she says. "They didn't start out as GRC solutions. They're not purpose-built for it. They were kind of just added on, and so they fall short of what GRC clients are looking for."

As Tarchinski-Krzoska points out, an alternate route might be to use an ITRC platform's own module to integrate with an ITSM tool.

"One of the features a lot of our customers like is that we also integrate with ticketing systems like JIRA and ServiceNow," she says. "You can open up a ticket directly within AuditBoard and it automatically syncs with the ticketing system, allowing for a two-way connection, so the ticketing system can be your source of truth for stakeholders, but AuditBoard can remain the single source of truth for your ITRC program.

An ITRC Platform Should:

- **Allow for IT governance, risk and compliance management**
- **Connect across the different GRC teams (audit & risk)**
- **Automate throughout the compliance lifecycle (audit planning, execution, external audits, ongoing compliance)**

Key features to look for:

- Integrated Platform
- Requirements Management
- Control Management
- IT Risk Management
- Assessment Management
- Policy Management
- Issue Management
- Project Management
- Reporting Capabilities
- Integrated Automations

Preparing Your Organization

Even though most modern ITRC platforms are SaaS (software-as-a-service) solutions, there's still a fair amount of preparation an organization must do before implementing one.

With any new software, that means change management, says AuditBoard's Tarchinski-Krzoska. It's something that's different and takes time both to implement and to get your team acclimated. "A lot of the time, people will revert back to manual ways because change is scary," she adds.

The chief principle, perhaps counterintuitively, is to not put technology first.

"Technology should be the last decision. And for many organizations, it's the first decision because it's easy. 'We'll buy the bright, shiny thing that's going to fix our GRC problem'," says Rica. "Ideally, what you want to do is build the organization, understand the assets, understand the controls, understand your risk tolerance and then go look for a technology that best matches up to your requirements."

The first thing to do is to perform a thorough self-assessment. Document your organization's processes, assets, known vulnerabilities, existing frameworks and controls. Then prioritize accordingly.

"I would probably do a crown-jewels risk assessment — 'Hey, what are the things that are most critical and most important to us?' Let's start there," says Rica, adding, "this can be a year, 12 to 18-month journey."

You also need to determine whether you have adequate budget and personnel to run the ITRC platform.

Lexmark's Willett says a prerequisite is an existing GRC process, even if it's one that still uses pencil and paper. Without that framework in place, he warns, adopting an ITRC platform may be fruitless.

"Before they go and adopt a platform, they better have a process already set up around risk and compliance, and really around governance, risk and compliance," he says. "If that's not already operating, if that process isn't starting to hum along, I don't feel that making the investment is worth doing at all. But when you do make the investment, don't understaff it. It is a project, and you need to treat it as such."

Pacific Western Bank's Creekmore stresses education for your staff well before an ITRC platform is implemented — and to select and additionally train ITRC "champions" who will run point on using the platform and train others.

"If you try to roll out an enterprise GRC platform to 3,000 employees, for example, you better have put the work in months ahead to educate them," he says. "You may have six or seven people in your organization who really understand governance, risk and compliance. And you have to find a way for them to be able to bootstrap, champion and successfully lead the adoption of an enterprise-class information system."

Selling an ITRC Platform to Executive Leadership

One of the trickiest parts of preparing to purchase and implement an ITRC platform is getting buy-in from the C-suite.

> ***"If you try to roll out an enterprise GRC platform to 3,000 employees, you better have put the work in months ahead to educate them."***
>
> — Dr. Jonathan Creekmore | *VP, Information Security Manager, Pacific Western Bank*

Rica recommends trying to change the way executives view GRC programs.

"We try to shift the conversation from, 'It's not a life insurance policy, it's a business enabler. This can make your business go faster; you can be bigger, stronger,'" he says. "You'll spend less time testing controls; you'll spend less time being compliant; you'll be able to do things that you couldn't do before because you have controls in place."

Patteson suggests sharing examples of concrete threats to prompt executives to take action — a notable data breach, the latest ransomware attack statistics or a new round of regulations.

"Folks don't go out and buy a governance, risk and compliance platform until there's a compelling event," he says. "The best way I've seen to justify these types of things to executives is really showing what that exposure is, especially if it's regulatory compliance."

As Smith notes, there are currently so many frightening cyberattacks in the news that getting buy-in might not be that difficult.

Features and Functions to Prioritize When Shopping for an ITRC Platform

You've decided to invest in an ITRC management platform; you've gotten the top brass to sign off on it, and you've performed the self-assessments and prepared the staff. Which features and functions should you be looking for in a modern ITRC platform?

The first is controls management. Many frameworks and regulations have very similar requirements, and you don't want to be testing and assessing the same control two or three times as a result.

"In many cases, there's a lot of overlap across frameworks," says Tarchinski-Krzoska. "You want the ability to manage your controls better, so as to not duplicate controls from multiple frameworks."

You also want the ITRC platform to be able to tap into a centralized repository of up-to-date regulations and requirements. Willett calls this a "dictionary" and Karp calls it a "central source of truth," but to Smith it's "just a consolidated area where I can see all the latest information and changes within the industry."

As new regulations come down or laws are passed, Tarchinski-Krzoska says AuditBoard's trusted content providers do the heavy lifting of updating requirements and adding them into AuditBoard so customers can focus their time on gaps and how to comply with the updates, not manually bring them into programs.

You'll want an ITRC platform that can integrate with your existing tools. We've already addressed ITSM incompatibilities, but you'll also want to consider integrations with configuration-management databases (CMDBs) and security-scoring services.

Ideally, your ITRC solution should be able to capture data and telemetry, generate compliance reports and a risk score while also suggesting and tracking remediation efforts.

Because many third-party risk assessments still depend on manually answered questionnaires, Willett suggests looking for a feature that will automate the distribution and processing of questionnaires as much as possible.

Watch for Future Developments

As the ITRC platform market expands and matures in the coming years, it might be worthwhile looking for new features in ITRC platforms that might not have been developed before this report.

"I should be able to feed it all policies, procedures, standards and it should be able to use machine learning and AI, like custom modeling and data science, to analyze qualitatively all of our GRC P&Ps [policies and procedures] to identify overlaps, inconsistencies and redundancies," says Creekmore.

Willett looks forward to greater integration of artificial intelligence in GRC platforms. "I hope that there are AI features coming soon that would help us be more efficient in running this process," he says.

With the changing landscape, it is not only important that GRC platforms innovate at a rapid speed, but that the innovations are in line with the demands of industries, allowing users to manage IT GRC programs through a risk lens.

What to Ask ITRC Vendors

In addition to the list of features and functions, there are several things you'll want to ask potential ITRC platform providers before you sign a service contract, such as:

- **What is the overall longevity of the product?**
- **What do you see happening with this service in the future?**
- **What's my return on investment from the product?**
- **How does your implementation process work?**
- **What is your post-implementation service model?**
- **How will you make it easy to integrate with an ITSM platform?**
- **How will you make it easy for me to import data, track activities and all those things we talked about in the integration?**
- **How do you tie your risk register to your controls, frameworks, issues and audits?**

Karp recommends asking pointed questions about how the ITRC platform can help consolidate GRC-related collaboration within your organization.

"How IT compliance partners with audit and risk [teams] should be a key part of what you're thinking about when you're reviewing any solution," Tarchinski-Krzoska says. "And if they don't have a good answer for how they'll bring those three teams together, then that should be a concern."

Additionally, as complexity continues to rise, it is imperative that, when evaluating different solutions, people consider it essential to be able to tie the risk register to controls, frameworks, issues, and audits — commonly through IT Risk Management solutions.

Finally, find out if the ITRC platform provider will help you set up the software during the initial implementation — and what the long-term service relationship will be.

"Don't just buy the platform," says Willett. "Make sure you get a partner that's going to help you set it up and get it configured."

Deployment and Optimization

Even when your ITRC platform of choice is a SaaS solution, you'll still have to implement and optimize it wisely. A slow, steady, phased-in approach might be best, beginning with the most critical parts of the organization.

"I would start with my most important data, my most important assets, my most important processes," says Rica. "Then I would continue to expand and bring other systems into the GRC platform over time, and I would continue to try to get as much automation out of it as I can."

Willett recommends working with the service provider to optimize the platform for your organization — and vice versa.

Over the long term, you will need to keep fine-tuning the platform as the regulatory and threat landscape changes along with your business. Continually assess the platform itself and how much return on investment you get from it.

But the real savings to be had, in terms of time and money, still lie with automation.

"Just keep trying to automate, automate, automate as much as [you] can," says Rica. "That's where you get the cost savings and the efficiency and the higher-quality results from a platform."

However, remember that IT governance, risk management and compliance ultimately come down to the humans running and participating in the program.

"You're only as strong as your weakest link in your initiative or effort," says Creekmore. "And risk management or GRC is definitely a team effort, all the way down to the lowest denominator or the common layman."

Once you get your ITRC management platform up and running, the benefits will soon be apparent. The streamlining, centralization, automation and thoroughness offered by the platform will result in your organization becoming more efficient, more compliant and more secure.

SPONSORED BY

AUDITBOARD

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fourth year in a row as one of the fastest-growing technology companies in North America by Deloitte.

To learn more, visit: AuditBoard.com

MASTHEAD

EDITORIAL

VP OF CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

PROJECT MANAGER

Victor Thomas | victor.thomas@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com

Security Compliance, Accelerated.

Simplify and scale your compliance program with a platform that unifies SOC 2, ISO 2700x, NIST, CMMC, PCI DSS, and more across your organization.

- **Scale Quickly**
  Automatically map new requirements to your existing controls to reduce manual efforts by linking requirements, risks, and controls.
- **Reduce Duplicative Work**
  Leverage the common controls crosswalk to visualize the overlap across frameworks and avoid audit fatigue.
- **Eliminate Manual Evidence Collection**
  Connect directly with your source systems to obtain the needed information and consolidate requests.
- **Track Issues in Real Time**
  Get visibility into identified issues, gaps, vulnerabilities, and action plans with dashboards and powerful reporting tools.

Top 100
Software Products
BEST SOFTWARE AWARDS
2023

Top-Rated by Customers

g2.com

★★★★½

Visit **auditboard.com/product/compliance-control** to learn more.

AUDITBOARD