RiskOptics

WHITE PAPER

Compliance Does Not Equal Security:

HOW TO TAKE A PROACTIVE APPROACH TO SEE, UNDERSTAND AND ACT ON RISK

CHASSERAE COYNE, Technical Product Manager

In recent years, a confluence of circumstances has led to a sharp rise in IT risk for many organizations. Cloud adoption, digital processes, remote work and third-party relationships have all grown dramatically to create an expanding and complex threat landscape that bad actors are eager to exploit.

Not only are there an enormous number of risks in this digitized world, but they are also coming at us at incredible speed. Considering that it only takes an independent cybercriminal around 9.5 hours to obtain illicit access to a target's network, every minute a company lacks visibility or fails to respond gives hackers a chance to cause significant damage.[1]

That's why a proactive approach to seeing, understanding and acting on risk is key to improving the effectiveness of defenses: It helps organizations enhance cyber resilience today and tackle the challenges of tomorrow.

The pace and scale of change, however, often leave information security leaders playing defense. They're looking for ways to get ahead of the game by improving:

ENABLEMENT: Supporting business goals by protecting the data and systems essential to the business.

EFFICIENCY: Eliminating the time wasted on manual tasks.

SECURITY: Protecting data privacy, demonstrating compliance, and managing risk effectively.

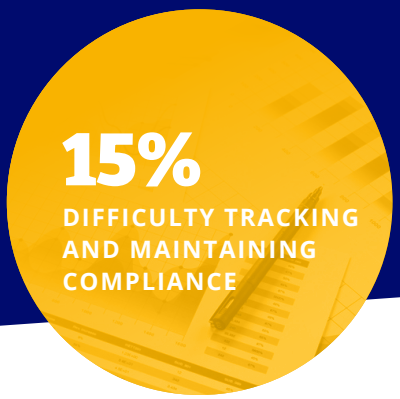
TRUST: Proving to customers that they can entrust their sensitive data to the company.

1 The Importance Of Time And Speed In Cybersecurity (forbes.com)

WHY ARE THEY HAVING DIFFICULTY ACHIEVING THESE OBJECTIVES? In a 2021 survey of CIOs,[2] respondents cited numerous challenges that made their governance, risk and compliance (GRC) efforts difficult in today's environment. Three, in particular, keep them up at night.

20%
NEW AND CHANGING REGULATIONS

40%
LIMITED RESOURCES AND BUDGET



15%
DIFFICULTY TRACKING AND MAINTAINING COMPLIANCE

SO HOW CAN ORGANIZATIONS BEEF UP THEIR CYBERSECURITY GAME? By taking a broader, risk-based approach that ties risk to business outcomes instead of a more limiting compliance-based approach. In this white paper, we'll look at how security leaders can make that happen with a modern risk management platform.

2 Today's CIO Imperative: Driving Greater GRC Efficiencies, Reciprocity, 2021

Where do we start?

Compliance is the typical starting point in protecting your organization. After all, it's a "must-do," and failure to comply can result in fines and other regulatory action. But focusing exclusively on compliance can leave you short-sighted and expose you to risk.

COMPLIANCE TYPICALLY RELIES ON MANUAL PROCESSES. You may find that it takes too long to start an audit, and you may be looking for ways to make this process more efficient and earn quick wins to prove value to the rest of the organization.

EVOLVING FROM A COMPLIANCE-BASED APPROACH TO A RISK-BASED one is a matter of shifting perspective. Compliance and risk are essentially two sides of the same coin, but with different focal points. Compliance is focused on adherence to a framework of statutory, regulatory, or contractual requirements, using implemented controls to satisfy those obligations. This adherence is binary — each requirement is either met or unmet.

BY CONTRAST, RISK IS FOCUSED ON MANAGING UNCERTAINTY with processes designed to achieve positive business outcomes. Risk is measured on a continuum, and whether a risk is acceptable will vary with an organization's risk appetite.

A MODERN RISK MANAGEMENT PLATFORM can build on your existing compliance efforts by incorporating them into standard frameworks that reduce uncertainty. The platform automates manual tasks, freeing resources and time to address more complex tasks. And it allows you to report on risk in the context of business objectives in a way that helps the C-suite and Board understand its value. Relating risk and compliance to business goals can drive strategic conversations and decisions about security.

Compliance alone is insufficient

"Being compliant" means adhering to a specific framework or list of regulatory requirements. It does not mean you have done everything within reason to protect your organization, nor are you prioritizing your security investments to achieve specific business objectives.

COMPLYING WITH A FRAMEWORK IS HOW YOU PROTECT YOUR ORGANIZATION, NOT HOW WELL YOU'RE DOING SO.

For example, compliance audits are point-in-time assessments that appraise the controls you've already implemented. They don't focus on how well you are protecting your organization today. This approach is no longer sufficient to reduce risk. What happens if an event occurs the day after an audit that increases your number of high-risk vulnerabilities? Remember that attackers don't care if you're compliant or not – only regulators and other stakeholders do.

The attacker aims to make money accessing your high-value information, disrupting your business, and profiting from ransomware payments. Attackers are smart, stealthy, and ready to exploit any opportunity, whether through the front door with a phishing email or the back door via one of your third- or fourth-party vendors. In fact, 83% of organizations reported having experienced more than one data breach, according to the 2022 Cost of a Data Breach Report by IBM and the Ponemon Institute.

SECURITY LEADERS ARE ALL TOO AWARE OF THIS SITUATION. According to Forrester, just 35% believe that compliance drives the right focus and behaviors within their business. They recognize compliance isn't forward-looking and risk can instantly impact the organization.

AS A RESULT, GRC BUDGETS ARE GROWING as risk management is perceived as value-add. In fact, 59% of security leaders plan to increase investment in risk and compliance technology, citing risk management as a business priority almost twice as often as compliance.[3]

3 Forrester Infographic: Risk Surpasses Compliance As Main Driver Of GRC Tech | Forrester, February 2022

4 ways that a modern risk management platform can strengthen compliance, reduce risk and accelerate business priorities

Understanding the need to shift from compliance to risk management is one thing, but carrying it out is quite another. When choosing technology, it's important that the platform supports a strategy of defining risk within a business context.

Let's look at the benefits a modern risk management platform can provide and the feature sets that enable them.

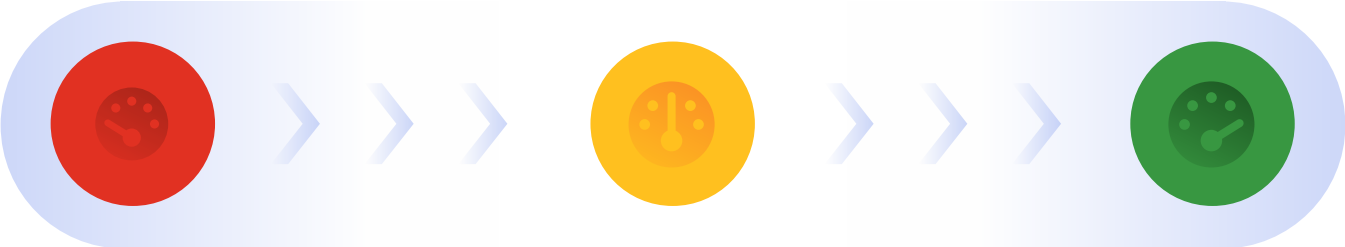
1. GAIN HIGH-LEVEL INSIGHT INTO YOUR COMPLIANCE AND RISK POSTURE IN A BUSINESS CONTEXT

By managing risk in the context of your business priorities, you can break down silos and eliminate gaps and blind spots. Look for a simple onboarding process that proactively recommends cyber assurance programs (CAPs) applicable to your business. CAPs unify risk observation, assessment and remediation activities around a business priority, such as cloud environments, protected health information (PHI), and retail operations. CAPs help ensure that the organization remains focused on its specific goals and that you can report on risk in a way that connects to these business goals. This, in turn, provides actionable insight into the risk implications of business priorities.

Your solution should recommend programs based on your industry, the markets you operate in, the type of data you manage, where data is stored, and other considerations. Programs unify compliance and risk (including third-party risk) into a single view around your business priorities. As a result, you gain visibility into how your compliance activities reduce IT and cyber risk so you can better prioritize critical opportunities for risk reduction.

2. AUTOMATE MANUAL WORK

Automation is key when data is constantly flowing from hundreds of systems. Given the complexity of integrating automation into business processes, it may make the most sense to take a "crawl, walk, run" approach.



WORKLOAD MANAGEMENT AUTOMATION, SUCH AS AUDIT EVIDENCE REQUESTS AND ISSUE TRACKING, IS A GOOD FIRST "CRAWL" FORWARD. The ability to schedule recurring tasks, reminders and follow-up items and report status enables some quick wins on your journey.

THE NEXT STEP ("WALK") IS A BIT MORE COMPLEX: automating inherent risk scoring and determining the inherent risk of working with third parties. This process begins by defining a common inherent risk calculation and risk appetite thresholds. Once set, you can utilize starting inherent risk scores created by experts and/or pulled in via integrations to third-party providers. This saves hours of work and the significant cost of consultants to determine the inherent risk.

As you're doing this, consider how your third-party vendors impact your risk. You can quickly vet third parties using data from third-party security ratings and assessment programs, rather than standard questionnaires, which can be inefficient or ineffective. According to Gartner, only 17% of organizations use all of the information they collect, while one out of four organizations review less than 60% of the information it collects.[4]

FINALLY, YOU'RE READY TO "RUN" BY MONITORING CONTROLS more frequently (and ideally, continuously). At this stage, you can eliminate manual, tedious work and increase accuracy with automated, cross-object risk scoring. This automation can help keep your residual risk current and eliminate risk blind spots across all your programs and activities. In addition, you can automate workflows for assessments and treatment to ensure work gets done on time and enable rapid response and remediation.

4 Gartner, *How to Prepare a Third-Party Risk Management Framework*, Legal and Compliance Research Team, 28 September 2021

AUTOMATION CAPABILITIES TO LOOK FOR IN A RISK MANAGEMENT PLATFORM INCLUDE:

- Guided program recommendations to speed onboarding.
- A unified taxonomy and data model that automatically creates relationships among controls, requirements, risks and threats, enabling data sharing and reuse.
- In-application guidance to help you scope requirements and controls, as well as generate required evidence collection templates.
- Integrations with external sources to automate evidence collection, speed collection and reduce errors by ensuring you have the right information to determine control effectiveness.
- Automated workflows for tasks such as risk assessments and automated cross-object scoring for an updated view of the risk and compliance posture of business priorities
- Real-time notifications to alert you to changes that negatively impact your risk posture, so you can act quickly when controls fail or risk exceeds your business's risk appetite.

3. UNDERSTAND THE EFFECTIVENESS OF YOUR COMPLIANCE AND RISK ACTIVITIES

Your risk management platform should provide information beyond the typical compliance status report. The real question is: How well are we protecting our organization and assets? Look for reporting capabilities that provide the context necessary to understand the progress and effectiveness of your compliance programs and their impact on reducing risk.

For example, each program should have a compliance posture indicating the number of effective controls compared to total controls. The platform should be able to update this metric in real time as your team completes compliance activities to provide an up-to-the-minute snapshot of the program's health.

You should also expect live-view dashboards to include the status and impact of controls and risks, as well as the ability to export results into a CSV or formatted report. This level of detailed reporting gives your risk managers the visibility they need to prioritize activities that strengthen compliance and reduce risk. For example, a risk assessment progression report could help you better understand how risk remediation efforts are progressing. Similarly, a report that quantifies risk assessments by category and score can help identify the risk categories needing attention, so that you can focus your resources on the areas negatively impacting your risk posture.

4. DEMONSTRATE THE VALUE OF INFOSEC ACTIVITIES TO EXECUTIVES

One of the most powerful benefits of a modern risk management platform is that it helps everyone consider risk in the context of business results. By defining and quantifying cybersecurity risk and investment value at the business unit, project and outcome level, the platform provides value by helping drive faster, data-driven decisions. Quickly identifying risks — both critical and those that exceed the organization's risk appetite — can help you prioritize activities and investments to reduce your risk exposure and strengthen compliance. This allows the CIO or CISO to demonstrate how reducing risk will help to safely accelerate business objectives. This also highlights the value of InfoSec activity and any needed investments, and clearly demonstrates the ROI to Executives and the Board.

The RiskOptics ROAR Platform helps deliver better business outcomes with less effort

RiskOptics ROAR is a cybersecurity risk management platform unifying risk observation, assessment and remediation. ROAR is more than a risk-management platform: It's an extra member of your team.

REDUCE WORKFORCE NEEDS. Automate mapping data to risk to triage the information constantly flowing from hundreds of systems faster and more cost-effectively than would be possible otherwise. Without automatically mapping data to risks, the workforce needed to triage the data would be cost-prohibitive.

SPEED PROGRAM STARTUP. Minimize program set-up time, effort and uncertainty by using a guided, content-rich approach that recommends programs and gets you up and running in under 30 minutes.

AUTOMATICALLY GAIN EXPERT GUIDANCE. In-application guidance helps you scope requirements and controls and automatically generates required evidence collection templates, reducing uncertainty and minimizing audit fatigue.

ELIMINATE MANUAL TASKS. Integrations and automated workflows for tasks, evidence collection, assessments and cross-object risk scoring eliminate tedious manual tasks, which frees up your team to do more valuable work.

ACCELERATE COMMUNICATION. Utilize risk monitoring to notify owners of changes to risks and related controls that have negatively impacted your risk posture.

In conclusion

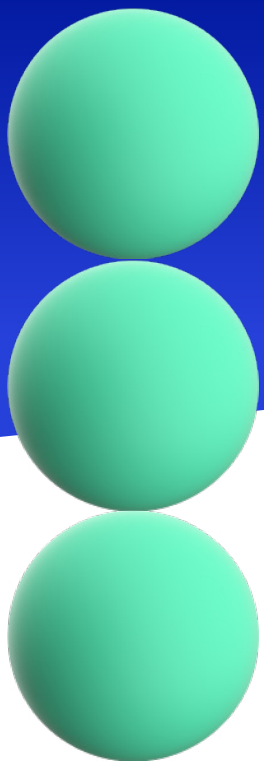
Cybersecurity leaders can deliver better outcomes with less effort by transitioning from a compliance-centric approach to a risk-centric one. Such an approach puts cyber risk in a business context so that CISOs and CIOs can tie risk to the business objectives prioritized by the C-suite and Board.

TO DO THAT, THEY NEED VISIBILITY into the organization's overall risk and compliance posture that breaks down the silos that cause inefficiencies, gaps, and blind spots. You need organizational and program-level reporting that gives you detailed insights and metrics. Automation capable of facilitating a continuous, near real-time view of the organization's risk profile is key to delivering better outcomes with less effort.

THE RISKOPTICS ROAR PLATFORM gives you the ability to see, understand and take action on your IT and cyber risks. With a unified, real-time view of risk and compliance —framed around your business priorities — you'll have the contextual insight needed to easily and clearly communicate with key stakeholders to make smart, strategic decisions that will protect your enterprise, systems and data, earning the trust of your customers, partners, and employees.

To learn more about the RiskOptics ROAR Platform

CLICK HERE



ABOUT RISKOPTICS

RiskOptics is the leader in IT risk management solutions, empowering organizations to convert risk into a strategic business advantage. The fully integrated and automated RiskOptics ROAR Platform provides a unified, real-time view of risk and compliance framed around business priorities, enabling CISOs and InfoSec teams to take a proactive approach to risk management.

RiskOptics customers are able to quantify the impact of risk on their business, communicate that impact to key stakeholders and mitigate expensive data breaches, system failures, lost opportunities and vulnerabilities across their own and third-party data while adhering to compliance requirements.

See Risk Differently

riskoptics.com

Copyright 2023 RiskOptics. All rights reserved.