RECIPROCITY®

WHITE PAPER

HAVE A STRONG COMPLIANCE PROGRAM? USE IT AS A FOUNDATION FOR RISK MANAGEMENT.

**Dave Schmoeller, GRC Expert
and Director of Solutions Marketing**

www.reciprocity.com

In the spring of 2020, organizations around the globe suddenly had a new reality: Stay-at-home orders meant that they had to shift their operating models overnight to accommodate employees, customers and suppliers working remotely.

The digital transformation many companies had planned over a period of years now had to happen in a matter of weeks or days. Respondents to a McKinsey survey published in the fall of 2020 say their company implemented key changes 20 to 25 times faster than expected[1].

Once the crisis abated somewhat, two things were clear. First, the changes implemented during the pandemic would be more or less permanent, and second, the threat surface was much larger than before the pandemic due to the increased number of remote workers on laptops, tablets, and phones. In fact, more than three in four (77%) respondents to EY's 2021 Global Information Security Survey say that they've seen an increase in the number of disruptive attacks, such as ransomware, over the last 12 months[2]. Yet in the consultancy's concurrent survey of corporate boards, just 9% declared themselves "extremely confident" that the cybersecurity risks and mitigation measures presented to them can protect the organization from major cyber-attacks[3].

Organizations around the world must all close this gap. But where to begin? If you have a compliance program, you are off to a great start. This white paper will show you how your information security program provides a foundation for a sophisticated and effective IT risk program.

Compliance and risk: What's the difference?

Compliance and risk often are thought of as separate, and in larger organizations they are distinct functions. However, upon deeper examination you'll see that compliance affects risk, and risk affects compliance; what you do within your compliance program directly impacts risk. In a sense they are *two sides of the same coin*.

Compliance consists of a framework of statutory, regulatory or contractual requirements and implemented controls to satisfy those obligations. Compliance is binary. Each requirement is either met or unmet.

Risk manages decisions across a range of expectations and actions to achieve positive business outcomes. Risk is on a continuum. Whether a risk is acceptable or not will vary with an organization's risk appetite.

[1] COVID-19 digital transformation & technology | McKinsey →
[2] Cybersecurity: How do you rise above the waves of a perfect storm? | EY - Global →
[3] Global Board Risk Survey | EY - US →

The top three challenges that security leaders face today

In a 2021 survey of CIOs[4], 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.

Limited resources (42%). Responding to risk is resource intensive. Few organizations had all the resources and budget necessary to adapt to changes that the pandemic response required. While budgets may well grow in the face of greater board and C-suite risk awareness, these security leaders recognize that they must eliminate inefficiencies and time wasted on manual tasks. These included creating new content, scoring and re-scoring risk, gathering evidence of controls, and tracking and reporting risk and compliance posture.

New or changing regulations (19%). The global compliance environment is becoming increasingly complex. Entirely new areas, such as data control and privacy, are growing in significance. And as organizations expand into new geographic markets, they face fresh new regulations. Businesses need to make sure that they're on top of compliance and that they're managing risk so that nothing critical falls through the cracks.

Tracking and maintaining compliance (15%). Finally, greater volume and complexity of compliance makes it increasingly difficult to manually create, assign, and gather evidence to demonstrate that controls are designed and operating effectively against compliance requirements.

Many organizations face all three challenges simultaneously, exacerbating an already difficult calling to effectively manage information security, risk and compliance.

Leveraging risk management principles drives better security because putting more resources toward reducing the highest risks more effectively safeguards business data and assets. The tools and automation involved can substantially ease the burden of managing this information and related activities. In addition, a risk management approach builds trust among customers and business partners, ultimately supporting your go-to-market initiatives.

[4] Today's CIO Imperative: Driving Greater GRC Efficiencies, Reciprocity, 2021 →

How to build a mature risk program rapidly

As your compliance demands expand and become more complex, it's hard to prioritize where to invest resources to respond to growing requirements. A better information security program moves on from "check-the-box compliance" to thinking more about **risk and business context**. That includes **how compliance activities impact the broader organization and its strategic direction and goals**.

Step 1: Start with compliance to build a risk management program

In a compliance program, controls are simply pass-fail. When the organization is "in compliance," it has met the minimum requirements under its obligations. But being able to say "we're compliant" is not the same as understanding to what extent implemented controls have effectively reduced the underlying risks. Compliance programs can be the foundation for establishing effective risk management with just a little more effort.

Taking a risk-centric approach requires asking these additional questions:

- Are controls effective?
- Do controls also contribute to achieving operational goals?
- Do controls help reduce risk?

To begin building a risk program, start with the controls. Recall that controls and risks are two sides of the same coin. Controls are just risks written from an opposite perspective. So, flip around the language of the controls and begin to uncover the underlying and related risks the controls are reducing. The result of this exercise will be a risk registry that you can further refine, categorize by business objective, and prioritize risks to bring them within acceptable limits.

Let's take a hypothetical example. Say a security policy requires users to create an eight-character password containing upper and lower case, numbers, and symbols. What is the risk behind this requirement? It's that a brute-force or other attack will be able to unlock a password and gain entry to your organization's systems.

By identifying the underlying risk, you can better understand how well this control addresses it and what actions are next (extend the length, limit login attempts, etc.) to lower the risk to an acceptable level.

Step 2: Build a better InfoSec program

A risk registry is a good starting point, but it's only the beginning. Standard registries focus broadly on all the things that can go wrong. Looking at risk from a holistic perspective is too broad and not really actionable. Different aspects of the organization may require different registries, scoring methods or both. Your organization needs to see exactly what is impacting its compliance and risk posture. Therefore, you must identify, assess, and monitor risk at a more granular level, such as by business priority or objective.

In addition, the relationships among requirements, controls, risks and threats are critical. If something happens in one area that impacts another (e.g., control failure increases the residual risk of the related business process), risk owners must be aware of the changes so they can take appropriate actions. Your organization should monitor risks and controls on a continuous basis, and exchange information among IT security, IT risk, IT compliance, and business owners.

InfoSec leaders need to focus more on risk implications within the business-driven context when making strategic decisions on information security and compliance.

Here's how to do that:

Focus on existing business activities: Consider your operations and processes, and consider how each one incurs risk.

Stay on top of risk: Once fully prioritized, your risk registry can guide your monitoring approach. Reserve continuous monitoring for your higher risks and key threats and controls. For lesser risks, periodic or occasional monitoring may suffice. Look for a solution that offers a consolidated view of relevant risks, controls and threats. In addition, the solution should automate the exchange of information (status, weighting, scores, etc.) among stakeholders to enable full-time and continuous monitoring of the organization's risk posture.

Share information seamlessly: Controls sit at the center of this data-sharing. Exchanging information between risk and compliance will bolster both functions in support of business priorities.

Step 3: Think strategically

The next level of maturity in a risk management program is to evolve from compliance tactics to risk strategy. Compliance measures the controls that are in place already, whereas risk management considers where the organization wants to go and what decisions it must make to get there. Risk focuses on understanding the risk implications of various investment options to minimize risks and be in a better position to succeed.

Because of its strategic stance, successful risk management requires buy-in at the executive level, as well as a place at the table for security executives during strategic decision-making. Considering risk once a decision has been made (or worse, executed) is simply too late.

The strategic level is also where the organization determines its risk appetite – that is, which risks it is willing to accept to achieve its goals and which ones it is not. This is a subjective judgment, of course, and the organization's leaders must determine what makes sense in the context of strategic and operational priorities. A tech startup will likely accept greater risk than an established financial institution, for example. Here are the questions to ask to gauge risk appetite:

- What is the opportunity before us?
- What risks does it create? What risks is it subject to?
- What investments are necessary to bring that risk down to an acceptable level?
- Is that cost significantly less than the opportunity?

If the answer to the last question is "yes," then the organization is better positioned to pursue the opportunity. If not, you must find other ways to reduce the risk or simply move on.

4 principles for better risk decisions

1 **Accept no unnecessary risk.** For example, it may be efficient to give full access to your systems and applications to everyone, but it's not necessary. Most people don't need access to all the data and all of the applications in your organization to get their job done, and doing so creates unnecessary risk that is easy to avoid.

2 **Make risk decisions at the appropriate level.** Whoever makes decisions should fully understand the risk and be able to allocate the resources to reduce it.

3 **Weigh the benefits and the cost to reduce risk.** The cost of mitigation must be significantly less than the opportunity it facilitates.

4 **Anticipate and manage risk by being prepared.** Should a risk event occur, the organization must have an appropriate action plan ready to deploy.

Step 4: Implement the program

The No. 1 reason to have a risk management program is to enable better decision making that avoids unnecessary risk, mitigates business exposure, protects valuable information, and optimizes information security. Decision makers and executive teams seek to understand what their compliance and risk postures are, so they can make better operational and strategic decisions. To achieve that goal, security leaders should work with stakeholders to implement a risk program, starting with deliberate planning.

Here are the five key stages of risk program implementation:

Planning. As we've discussed, compliance and governance structure is the best place to start. What components of these can you leverage for a risk program? What kind of structure should you use? Consider the compliance and security programs already in place. How can you use these to build a formal risk management program quickly, without starting from scratch? What existing communication channels can you use to talk about risk to get everyone on the same page? And finally, what will governance and oversight look like? If a compliance or governance committee is in place, can it just expand its scope to include risk management?

Involvement. InfoSec leaders are already performing security awareness training across the organization with the message that security is everyone's responsibility. This is an ideal opportunity to introduce the concept of risk and share materials on risk management practices, risk and vulnerability identification, and concepts around remediation. The new message: Risk is everyone's responsibility.

Identification and analysis. As noted above, risks should align with the business processes and objectives that create them. Beyond that, define IT risk program structure, common language, and scoring methodology. Then, communicate them across the organization in order to evaluate and score risks consistently and within the appropriate business context.

Remediation. As you identify and analyze risks, what gaps exist? Apply the guiding principles [see sidebar] to evaluate gaps and opportunities for remediation. Perhaps a control isn't in place, or it's not operating effectively. Set a target risk score and work to close the gap between the inherent risk and the target risk.

Preparedness. Even if you do your best to manage risks, there's always the chance that a risk event will occur. Preparing your organization with business continuity planning and disaster recovery exercises as part of compliance programs will put you ahead of the game.

InfoSec Best Practices

Accountability: Risk is everyone's responsibility. Connect diverse teams with risk education, common program structure and common taxonomy to facilitate ownership of risk at the appropriate business level.

Leadership: It is critical to set the example, tone, and culture of risk in the organization.

Timeliness: Conduct regular risk assessments. Score and rescore risks based on updated or new information across the business.

Quantification. Quantify and prioritize your risks on an ongoing basis to fully understand where to focus your investments.

Implementation: Implement program governance and take action on risk treatments including strong controls.

Driving business results with a strategic approach to risk

Every business activity involves risk, so simply viewing and measuring risk at a high level is not enough. You must also identify and categorize risks as they relate to individual business activities and the context around them. Managing risk is all about delivering insights so that executives and the board can better understand their IT risk posture and use that knowledge to make better decisions.

The Reciprocity Product Suite delivers a single, real-time view of risk in context of your business activities empowering security teams and business teams with the actionable insights needed to avoid and mitigate risk and optimize information security.

Using an AI-powered approach, the Reciprocity ROAR Platform unifies your organization's risk observation, assessment, and remediation activities with a single, real-time view of risk and compliance in business context. It offers actionable insights so you can focus resources on reducing the risks behind your organization's critical strategic objectives and achieve positive outcomes.

Reciprocity ROAR Platform

Strategic IT risk management framed around your business priorities

DISCOVER THE POWER

ABOUT RECIPROCITY

Reciprocity is pioneering a first-of-its-kind approach to IT risk management that ties an organization's risk directly to its business strategy.

The fully integrated and automated Reciprocity ROAR Platform, which underpins the Reciprocity ZenRisk and ZenComply applications, enables security executives to communicate the direct impact of risk on high-priority business initiatives to key stakeholders, helping them make smarter, more informed decisions.

With Reciprocity, InfoSec teams can strategically support their organization and foster company growth by optimizing resources and mitigating expensive data breaches, system failures, lost opportunities and vulnerabilities with their customers' data.

Security builds trust.

www.reciprocity.com