

Managing Complex Risks Across Teams

Corporate, Securities, and Governance



Banner artwork by *topvector / Shutterstock.com*

In today's evolving corporate landscape, organizations grapple with the intricacies of identifying and managing complex risks across the enterprise. In an environment where enterprise risks are expanding, the legal function's role in safeguarding the corporation has been heightened. Increasingly, corporate in-house legal teams are charged with overseeing risk management. The *2023 ACC Chief Legal Officers Survey* found, in addition to Legal, at least 20 percent of CLOs also oversee one or more of the following functions: compliance, privacy, ethics, risk, government affairs, ESG, and cybersecurity response. These risks extend across various departments, and while the legal team is strategically positioned to collaborate cross-functionally, effective management of risk across cross-functional teams can be a challenging undertaking.

A. Problem: Navigating complex risks across cross-functional teams

Silos undermine effective risk management. To properly identify risk, functions need to understand how different viewpoints affect risk assessment. A few examples of the cross-functional nature of complex risks include:

- ESG, encompassing environmental, social, and governance aspects, spans diverse activities and naturally requires cross-functional collaboration. For instance, social initiatives often fall under the purview of human resources, while governance typically aligns with legal. Environmental issues can be spread across the organization, and most often include supply chain, procurement or real estate.

- Cybersecurity: Traditionally, cybersecurity was the purview of the Chief Information Officer (CIO) or Chief Security Information Officer (CISO). As the importance of cybersecurity governance continues to grow, the reality is that effective management of cyber risks is far more cross-functional. Cybersecurity encompasses various teams, including engineering and development, legal and privacy, and compliance, all of which must come together during a security incident, making it an all-hands-on-deck situation.



Cross-functional teams play a tremendous role in working together to manage cybersecurity risks. Pavel Vinnik / *Shutterstock.com*

- Privacy: For many companies, privacy compliance originated with the legal team. Given the rapidly changing regulatory frameworks for managing privacy risks, sales, marketing, customer service, IT, and finance departments all regularly touch on various aspects of a privacy program.

  As the importance of cybersecurity governance continues to grow, the reality is that effective management of cyber risks is far more cross-functional.

Managing these types of risks within a single discipline runs the risk of developing a program that has not considered the various nuances of addressing a complex risk. But managing across functions to achieve a common goal is challenging. Cross-functional teams may have divergent goals or mismatched resources to designate for a particular issue. Coordinating across teams is best but may lead to a lack of ownership for a problem or lack of clarity about who can make decisions. Further, different teams may have diverse risk tolerance levels, which can make alignment difficult.

Coordinating across teams is best but may lead to a lack of ownership for a problem or lack of clarity about who can make decisions.

If a business does not resolve such challenges in getting their cross-functional teams aligned to manage the risks they face, they can increasingly get into trouble:

- Regulatory pressure and disclosure: Companies increasingly face mounting regulatory pressure to disclose risks and the strategies employed to mitigate them. For US based public companies, the new requirements from the Securities and Exchange Commission mandate further disclosure about how a company manages cyber risk. There is also expected rulemaking that may require added disclosure about ESG risks.
- Expanded duty of loyalty: Recently Delaware courts decisions have expanded the duty of

loyalty to require corporate directors and officers to maintain oversight over risk management systems for mission critical risks and key compliance risks. In cases like *Boeing* and *McDonald's*, the Delaware Chancery Courts have held that responsible officers must have a system for identifying risks and address "red flags" that result from such systems.

B. Solutions: Techniques for effective cross-functional risk management

There are many ways to bring cross-functional teams together to achieve a common goal. Here are some techniques that worked for us in helping bring teams together to manage risk and mature compliance programs.

Using a similar structure across multiple risk areas will start to feel familiar for different functional areas, which can make a buy-in on how to address multiple risk areas and can be customized to work within your company's culture.

- Apply the most effective techniques of your mature programs: Your most mature risk management can serve as a model for less mature areas. You may have a leading program that has been able to implement features like a risk register, Roles and Responsibility "RACI" charts, a committee oversight structure, or compliance framework. These are all programmatic elements that can be repeated to manage different risk areas and can be customized to work within your company's culture. Using a similar structure across multiple risk areas will start to feel familiar for different functional areas, which can make buy-in on how to address a new risk area easier to obtain. If your organization lacks a mature program to replicate, start by picking one to develop first. Get that one right and then roll it across the others.



Build a strong risk management structure that can be utilized across all departments. aurielaki / *Shutterstock.com*

For example, our transformation team developed a Power Business Intelligence (BI) project tracking dashboard and bi-weekly meeting cadence for reporting to management. They aided the maturity of our compliance program by giving it space on the dashboard and designated time for a report out at the meeting. Our cybersecurity team developed a model for tracking and graphically showing progress against a framework. This team helped privacy by adapting their model to show progress against a privacy framework. In our experience, the most mature programs in technology focused companies tend to be cybersecurity related, in part because of customer expectation for security certifications and diligence required by insurance companies to underwrite cybersecurity insurance coverage.

- Common frameworks: Encourage common frameworks recognized by cross-functional teams. This alignment simplifies communication and fosters a shared understanding of risk management strategies. For instance, the National Institute of Standards and Technology (NIST) publishes a Cybersecurity Framework that is widely adopted. NIST also has frameworks for privacy and risk management, handling government CUI, and a newly developed framework for AI risk management.

  Internationally, the International Organization for Standardization (ISO) is a well-known non-governmental entity that focuses on developing voluntary standards for quality management. ISO standards are wide ranging, but legal teams may be most familiar with ISO 27000 standards which cover information security and privacy protection or ISO 26000 which sets up frameworks for sustainability programs. For compliance programs, legal teams often use the "Seven Elements of an Effective Compliance Program" from Chapter 8 of the US Federal

Sentencing Guidelines," along with the US Department of Justice "Evaluation of Corporate Compliance Programs." By reporting against a common framework, or reporting on different frameworks using a similar format, different departments can gain visibility into the alignment of different efforts, in a manner that encourages harmonization.

- Clear lines of responsibility: Ensure that clear lines of responsibility are assigned to specific teams or individuals. This clarity enables streamlined risk management and reduces confusion regarding roles and expectations. If you have a framework, you can organize your cross-functional teams by assigning responsibility for the elements or controls of the framework.

- Project manager involvement: Appoint a dedicated project manager to oversee cross-functional risk management initiatives. This individual can serve as a central point of contact, facilitating communication, naming stakeholders, coordinating efforts, and ensuring that the various teams are working cohesively. Project managers can develop consistent reporting across different risk areas and can be charged with showing the consequences and likelihood of a risk area. Once the project manager can report on risk, this can be shared with other internal stakeholders, other risk committees, and executive management, including the board of directors.



A reliable project manager serves as the focal point in cross-functional risk management, while also communicating findings with other parties. eamesBot / *Shutterstock.com*

- Share information and build trust: In the era of remote work, you should pay attention to building trust amongst teams working together to manage the same risks. In-house legal teams can find new ways to share information across the organization and should consider

technology tools that can supply broader risk and control oversight.

Legal teams at the forefront

The challenges posed by complex risks can be daunting, but they are not insurmountable. Be intentional about fostering teamwork by actively seeking solutions that resonate with the unique dynamics of your organization. Mature risk management programs can offer a solid foundation, while adopting common frameworks can ensure alignment across teams. Clear lines of responsibility, the active involvement of project managers, and a culture of information sharing and trust are integral components that align teams toward a shared objective. By implementing such tried-and-true techniques, you can work with others within your company to navigate complex risks effectively.

Scrutiny of risk management and board oversight of risk management is on the rise, but a proactive and collaborative approach to risk management supported by the legal team is indispensable for the long-term success and resilience of any enterprise. Find solutions that work for your organization to work collaboratively to manage complex risk. Complexities can be overcome by applying techniques such as using mature risk management programs, adopting common frameworks, setting up clear lines of responsibility, involving project managers, and fostering information sharing to build trust helps align teams toward a common goal.

Join ACC

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its authors' employers, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Noah Webster



Chief Legal and Compliance Officer

Everbridge

Noah Webster is chief legal & compliance officer for Everbridge, a global software company that empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today’s unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry’s most comprehensive risk data to Keep People Safe and Organizations Running.

Cara Bradley



Deputy General Counsel

Everbridge

Cara Bradley is the deputy general counsel of Everbridge, Inc., a global software company that empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today’s unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry’s most comprehensive risk data to Keep People Safe and Organizations Running™

Bradley manages a legal team that handles commercial contract negotiations, public company compliance, human resources, mergers and acquisitions, global compliance, and business strategy for Everbridge.