Essential steps for building a successful integrated risk management program
**Introduction**

Although the term integrated risk management (IRM) is new, the concept is not. Gartner defines IRM as “a set of practices and processes supported by a risk-aware culture and enabling technologies that improves decision-making and performance through an integrated view of how well an organization manages its unique set of risks.”

The idea of an integrated view of risk is well-understood in heavily regulated industries like financial services, manufacturing, and healthcare. They have long had to prove compliance with a variety of regulations unique to different departments and functional groups such as SOX in finance, privacy regulations in legal, and NIST or HIPAA in security. This has forced many of these organizations to take a broader view of managing risk, even though piecing together a consolidated report of organizational risk for auditors, executive management, or the board has been time-consuming and painful. Newer regulations that aim to protect the data and privacy of citizens, such as the European Union’s General Data Protection Regulation (GDPR), have driven the need for a more integrated view of risk to include third-parties, other industries, and smaller organizations.

Legacy governance, risk, and compliance (GRC) tools, however, have not kept pace with the needs of the business or the demands and progression of technology as it relates to digital transformation. And many organizations have not built a foundation to support an organization-wide integrated risk management program.

**Three emerging domains of risk**

Enterprises face a host of risks (and some industries may be subject to one more than another), but generally speaking there are three domains of risks that enterprises must protect against:

1. **Cyber risks, including data breaches.** Nearly every board is watching this issue closely and directors want to know how customer, employee, intellectual property, financial, and operational data is being secured. The average cost of a data breach is in the millions of dollars, and the reputational or brand damage and loss of customers can be even more devastating, both to the bottom line and stock valuation.

2. **Regulatory failures.** Enterprises are being required to comply with increasingly strict regulations and legislation such as those governing the storage and handling of personal data. Over the last nine years, regulators have fined financial services businesses alone $342 billion for regulatory failures. This has erased an estimated $850 billion in profits for the top 50 global banks.1 Under the GDPR, breaches of compliance may incur penalties of up to 4% of global annual revenue and an enforced shutdown of EU operations.

3. **Third- or fourth-party risk.** This occurs when an enterprise interacts with other organizations, and those organizations deal with other parties on behalf of that enterprise. Boards and senior executive teams need to consider the implications of third or fourth parties operating in ways incompatible with their business’s values, culture, or regulatory obligations. This increasingly becomes an issue as more organizations outsource significant portions of their operations to third parties. Organizations sometimes fail to realize they can outsource operations but the liability and risks stay with the organization. Breaches involving third-parties are on average 12% more costly to remediate2, underscoring the need to continuously manage vendor risk.

Without a unified view across the organization, real-time identification and a coordinated response to these diverse and distributed risks would be nearly impossible.

---

1 Reuters: U.S., EU fines on banks’ misconduct to top $400 billion by 2020: report. September 27, 2017
2 Ponemon Institute Cost of a Data Breach report 2017
Creating a solid foundation

Before creating the practices and processes necessary for an integrated risk program, a solid foundation must be established. Once built, this foundation will support the organization’s strategy, people, processes, and technology.

The foundation is made up of four elements:

1. **A shared understanding of risk across an organization.** Create this through a common taxonomy and language. A single language for risk ensures chief financial officers, chief legal counsels, and chief information officers understand what constitutes a low, medium, or high risk to an organization and can respond accordingly. With that, everyone can work together to manage risk to comply with regulatory regimes, take advantage of new business opportunities, and operate more efficiently.

2. **A sound risk and compliance culture.** Risk is a driver of success—without risk, innovation stalls and the competitive edge is lost. An organization with a sound risk and compliance culture agrees upon an acceptable level of risk and, through continuous monitoring and prioritization, identifies and responds to risk effectively and consistently.

3. **Executive sponsorship.** For an organization-wide risk program to be successful it must be driven from the top by someone who has both spending power and board support.

4. **A single source of truth.** Everything must be built around a consolidated data source that provides context for risk prioritization, allows cross-functional automation, and ensures individuals organization-wide can visualize risk in a meaningful way.

With these foundational elements, businesses can evolve from managing compliance and risk with ad-hoc manual processes to managing risk at board level, applying common taxonomies and using technology to automate and visualize risk processes.
Building a successful integrated risk program

Once the foundational elements have been established, they must be tightly woven into an organization’s strategy, people, processes, and technology to become a natural part of the business.

**Strategy:** Establish and activate a risk-aware culture, sponsorship, plans, and roadmaps. This includes development and implementation of an IRM framework, and performance improvement through effective governance and risk ownership.

**People:** Empower everyone from leaders to individual contributors and give them the resources to perform their tasks. Communication and reporting are vital, and provisions must be made to implement the best and most appropriate means to track and inform stakeholders of an enterprise’s risk response.

**Processes:** Create processes that deliver risk and compliance outcomes and ensure teams, groups, and stakeholders can follow them. It is critical to identify and implement processes that methodically track governance objectives, risk ownership/accountability, compliance with policies and decisions that are set through the governance process, risks to those objectives, and the effectiveness of risk mitigation and controls.

**Technology:** Take advantage of technologies that accelerate strategy, establish processes, enable collaboration, drive engagement, support IRM strategies, and keep people informed and involved.

One platform serving as a single source of truth mitigates risk through continuous, consistent processes for monitoring and enforcing policies.

One platform serving as a single source of truth mitigates risk through continuous, consistent processes for monitoring and enforcing policies. Organization-wide monitoring, prioritization, and cross-functional automation drives better collaboration and decision-making to speed response. Reducing redundant and repetitive processes increases productivity and performance.
Conclusion
Building an integrated risk program requires commitment, a willingness to change, and the right partners and technology. It doesn’t happen overnight and takes time and effort to get buy-in throughout the company. But the rewards are substantial—lower operating costs, increased productivity, happier employees, better visibility and decision-making at all levels, competitive advantages, and reduced risk of a breach or non-compliance.

To get started:
1. Evaluate your current compliance and risk maturity (programs, processes, technology, etc.), level of commitment to change, and risk tolerance
2. Secure executive sponsorship and make the necessary changes to put the foundational elements in place
3. Ensure the foundational elements become core aspects of what makes your business successful (the strategy, people, processes, and technology)
4. Choose a place to start that will maximize your ROI (low effort and high impact): a regulation, department, or initiative

You’ll see immediate benefits, but the cumulative impact as the implementation matures and the program spreads throughout the enterprise is truly revolutionary.

ServiceNow enables your change
A new paradigm for managing risk is needed to deliver on the promise of integrated risk management. To understand the full scope of risk, organizations must gain a comprehensive view across all business units and risk and compliance functions, as well as key partners and suppliers.

Our cloud-based Now Platform® with a built-in CMDB functions as a single source of truth. It supports people-friendly processes, flexible workflows, role-based dashboards, and real-time visibility. And the ServiceNow portfolio of applications, partner ecosystem, and innovative integrations that can make your integrated risk management program a reality.

Learn More
Find out why ServiceNow was named a leader in Gartner’s 2018 Integrated Risk Management Magic Quadrant and learn how we can help you build a successful integrated risk management program.