WHITEPAPER

Why Your Nonexistent Risk Management Platform is Bad for Business

The cost of inaction in risk management and compliance is high. Organizations that fail to implement effective solutions risk significant financial and operational consequences. In this whitepaper, we explore ways to stay resilient, from the benefits of open versus closed platforms to choosing the right system, to avoid common pitfalls of non-compliance and inefficiency.

Did you know?

Organizations that adopt strategic risk management are five times more likely to build stakeholder confidence and achieve superior business results. Additionally, they are twice as likely to anticipate faster revenue growth.

The biggest risk now, say business leaders? Did you guess that cybersecurity is the number one business risk on managers' minds? In fact, a reported three in four managers say they remain worried about more frequent or broader cyber-attacks to come.

Cybersecurity, of course, is merely one risk example of so many. The overarching theme so matter the risk situation? Act. Don't merely react.

SAI360
RISK FROM EVERY ANGLE

Case in point? CrowdStrike.

The recent CrowdStrike disaster—a moment of truth for so many—is just one example of risk spreading like wildfire.

Some were shielded from organizational damage. For instance, several companies demonstrated preparedness for the CrowdStrike incident by having robust cybersecurity measures and proactive risk management strategies in place. These organizations had invested in advanced threat detection systems, regular security audits, and comprehensive incident response plans, enabling them to quickly identify and mitigate potential threats. By conducting frequent cybersecurity training for employees and maintaining an updated awareness of emerging threats, these companies strengthened their defenses against potential cyberoutages. Their proactive approach minimized the impact of the CrowdStrike breach. It also reinforced stakeholder confidence in their ability to manage risks effectively.

Businesses with up-to-date cybersecurity frameworks and regular incident response exercises could quickly identify and mitigate risks, ensuring operational stability. By maintaining agile incident response strategies and regularly updating their business continuity plans, these organizations effectively navigated the challenges posed by the CrowdStrike outage.

In short, it's truly a case of being prepared versus having to perform damage control after-the-fact.

The greatest lesson?

According to a Gartner survey, over 60 percent of companies believe they have integrated systems simply by centralizing data. However, without advanced analytics and collaboration, these systems miss critical insights, impacting strategic decision-making. The absence of ethics and compliance training further exacerbates compliance failures, leading to costly legal penalties.

Storing data is insufficient; organizations need systems that connect data across business units and provide deep analytical capabilities. Without this, companies risk being blindsided by threats that could have been mitigated or turned into opportunities.

A lack of integration has hidden costs, including inefficiencies and redundancies, such as duplicate processes and inconsistent data. These inefficiencies increase operational risks, like gaps in coverage and slower response times, leading to higher costs. Additionally, regulatory and compliance risks result in fines and legal penalties, more frequent and complicated audits, and misguided strategic decisions based on fragmented information.

Here's more on what to know now and strategies your organization can leverage to act versus react in the future.

There are Hidden Costs of Inaction

Organizations without integrated risk management solutions face substantial risks. Failing to manage risk effectively can lead to a range of costly consequences, including financial losses, reputational harm, and operational setbacks. These costs can extend beyond immediate financial impacts and may include:

- **Legal and Regulatory Challenges:** Fines, lawsuits, and other legal or regulatory actions.
- **Reputational Harm:** Diminished trust in the organization's ability to operate with integrity.
- **Operational Setbacks:** Project failures, delays, budget overruns, and dissatisfied clients.
- **Missed Opportunities:** Unrealized potential benefits and a decrease in market share.

Get ready, get set...here are three things to know now.

Your Blueprint For Success

1. Consider the Ever-Critical Open vs. Closed Platform Debate

Choosing the right risk management platform is critical for success and is one way to safeguard your organization. Organizations are increasingly evaluating the benefits of open versus closed systems to ensure they remain agile and responsive to changing conditions. Open platforms offer flexibility, allowing integration with various tools and systems, while closed platforms often lock organizations into specific ecosystems, limiting data accessibility and adaptability. Being LMS-agnostic is crucial for seamless data integration and accessibility, ensuring companies are not constrained by vendor-specific limitations.

Closed platforms, on the other hand, can create challenges by tying organizations to specific technologies or tools. This makes it difficult to adapt to changing business needs. For example, if a company uses a closed LMS, switching to a different system can be costly and complex, often requiring data migration and retraining of staff.

In contrast, open platforms offer greater flexibility, allowing businesses to choose the best tools for their needs and integrate them easily. This flexibility is essential in today's fast-paced business environment. Why? The ability to adapt quickly can provide a significant competitive advantage.

2. Be Careful to Choose the Right Vendor

Selecting the right vendor involves evaluating flexibility, integration capabilities, and support for organizational goals. On-premise solutions may seem secure. However, it's important to note that they often lack the agility and security of modern cloud-based systems. The Equifax data breach of 2017, for example, only highlighted the dangers of relying on outdated, on-premise systems. The importance of modern, integrated solutions became shockingly evident in that instance, and of course, for so many others.

A good vendor should offer robust integration capabilities, enabling seamless data flow across systems and departments. Additionally, they should provide ongoing support and training to ensure that the system is used effectively and that employees are equipped to handle complex compliance and risk management challenges.

When choosing a vendor, organizations should consider several key factors, though these are, of course, by no means exhaustive:

- **Vendor Experience in Your Industry:** A proven track record means higher understanding of personalized needs
- **Integration Capabilities:** Ensure a vendor can integrate seamlessly with your existing systems, particularly within an open or LMS-agnostic environment
- This is just a start. Every organization has unique requirements. A thorough evaluation should include a broader range of considerations tailored to your specific goals and challenges.organization needs

3. Leverage Modern, Integrated Solutions

True integration goes beyond simply storing data in centralized locations. It involves using advanced analytics and fostering cross-functional collaboration to gain actionable insights that drive strategic decision-making. By ensuring seamless data flow and accessibility across departments, organizations can improve performance and resilience, address risks effectively, and maintain a competitive edge.

Modern ethics and GRC solutions provide the tools necessary to navigate these challenges. They offer enhanced user interfaces, improved security measures, and continuous updates, ensuring compliance with industry standards and leveraging the latest technological advancements. By investing in these modern solutions, companies can reduce operational costs, increase efficiency, and drive growth.

FINAL THOUGHTS

Failing to adopt integrated platforms and proactive risk management strategies can lead to increased costs, legal penalties, and strategic blind spots. Organizations must prioritize the adoption of flexible, open systems that allow for adaptability in a dynamic business environment. The ability to integrate various tools and systems ensures that businesses can respond quickly to emerging challenges and opportunities.

To remain competitive, organizations must embrace platforms that enable strategic alignment and informed decision-making. By selecting the right solutions and vendors, businesses can protect themselves from the financial and operational consequences of non-compliance and inefficiency. Embracing modern, integrated platforms allows companies to make informed decisions, drive growth, and maintain a competitive advantage.

What should an ideal journey toward effective risk management and compliance look like? It's about recognizing the costs of inaction and understanding the benefits of modern, integrated solutions.

By prioritizing the right platforms and strategies, organizations can secure their future, mitigate risks, and capitalize on opportunities for success.

In a world where adaptability is key, choosing the right approach to risk management is essential for long-term success.

Interested in learning more about how your organization can execute a smart and strategic risk management platform?

Let's start a conversation.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360
RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.
Visit www.sai360.com.

175278 0824