IT Risk in Insurance:

10 Key Features Your Compliance Solution Needs

AUDITBOARD

In today's data-driven business environment, ineffective cyber risk management can pose a serious threat to achieving strategic business objectives. According to PwC's 2023 CEO Survey, **cyber risk ranks among the top three areas where insurance CEOs feel most financially exposed**, in addition to inflation and economic volatility. For insurance organizations, staying ahead of cyber risk should be a top priority to safeguard business growth and expansion opportunities.

For the 13th consecutive year, the United States had the **highest global average total cost** of a data breach at **USD 9.48 million**, according to IBM's 2023 Cost of a Data Breach Report. In addition to financial penalties and disruption to the business, cybersecurity breaches cause reputational damage that can seriously harm the business.

In addition, escalating IT compliance risk — exemplified by the recent passage of the SEC's new cybersecurity disclosure rules in the U.S. — further emphasizes the need for effective IT risk management to safeguard insurance companies from regulatory fines and reputational harm that can affect strategic business objectives.

In this article, we will explore the implications of these trends and regulatory signals in the insurance industry — and discuss practical steps insurance companies with a growth-oriented mindset can take to fortify their IT risk and compliance programs.

Amid Changing Regulations, Robust IT Risk and Compliance Is a Competitive Advantage

Since 2018, when the European Union's GDPR and California's Consumer Privacy Act went into effect, the regulatory landscape has continued to evolve at a rapid pace in response to rising cybersecurity threats across the globe.

> ***"71% of countries in the world** have adopted data protection and privacy legislation."*
>
> *— The United Nations Conference on Trade and Development*

IBM found that while 95% of studied organizations have experienced more than one breach, breached organizations were more likely to pass incident costs onto consumers (57%) than to increase security investments (51%). **This highlights the major opportunity for insurance companies to invest in strong IT risk and compliance programs as a competitive advantage.**

Growth-minded insurance firms are staying competitive by making investments in more stringent compliance programs, not only to protect themselves, but also to get ahead of barriers to entry into new markets like Europe and Asia. Gaining consumer trust through obtaining security certifications — e.g. SOC 2, ISO, and GDPR — is a high-value endeavor for businesses, perhaps even more so for insurers, given a large part of their business depends on the safe handling of sensitive customer information.

Slacking on regional compliance can have severe repercussions, not only for insurance companies, but for all industries. A recent example is the **$5 million fine that The New York Department of Financial Services imposed on Carnival Corporation** for multiple violations of the state's Cybersecurity Regulation (23 NYCRR Part 500). While $5 million is a hefty fee, it is only one aspect of the financial impact of a local violation; not included are the legal costs and the collateral reputational damage that can harm relationships with investors and customers.

It comes as no surprise that **67% of insurance CEOs named regulatory changes the biggest potential source of industry disruption**, according to PwC's 2023 CEO Survey. Given the sheer number of data privacy and cybersecurity requirements a business may be subject to — depending on its industry, state, country, and where it conducts business with its customers and third-party partners — staying on top of compliance requirements has become a major and necessary challenge for insurance companies.

The Growing Urgency of Effective IT Risk and Compliance Management in Insurance

The SEC's newly adopted cybersecurity disclosure rules — requiring public companies to disclose material cybersecurity incidents on a Form 8-K within four business days — **signal a new period where IT risk management is no longer an optional best practice but a mandate for public insurance companies.**

In addition, Item 106 requires registrants to **"describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats."** For public insurance companies, this essentially means:

1. **Governance:** A CISO must sit on the board of directors.
2. **Cyber risk management and strategy:** The board will need to quantify cybersecurity risk impacts to the business (in dollars).
3. **Cyber incident reporting:** Companies must describe the nature, scope, and timing of cyber incidents and their material impact — or reasonably likely material impact — on the business.

These new rules underscore the deepening intersection between cybersecurity, finance, and investor relations for public insurance companies. **The SEC has acknowledged the financial impact of cybersecurity breaches, and has required organizations, at the highest level, to take responsibility for the IT risk and security posture of their business.**

> *"Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors."*
>
> — SEC Chair Gary Gensler

Managing More IT Compliance Requirements With Efficiency

Cost-effectiveness and efficiency are predominant considerations when it comes to fortifying IT security programs, which require significant investment of resources, time, and technical expertise. At the same time, already lean-staffed risk and compliance teams are struggling to manage their existing workloads with available resources — necessitating action.

A potentially time and cost-saving best practice is to invest in technology that can help your IT risk and compliance teams more efficiently manage the growing volume of compliance requirements.

However, the last thing any executive wants is to invest in a full-suite GRC solution, only to have it shelved due to low user adoption, the time and expertise required to manage it, and numerous FTEs required to implement it — all while day-to-day risk and compliance processes continue to be performed manually. Based on feedback from our customers and sales research, the following are the top attributes to look for in your IT risk and compliance technology solution to save you from winding up in this scenario.

Top 10 Features Insurance Companies Should Seek In an IT Risk and Compliance Solution

1. **Self-servicing**
   The solution is designed with self-service in mind: it is no-code or low-code and has self-configuration options, allowing for easy user adoption and a lower total cost of ownership.

2. **Out-of-the-box framework mapping**
   The solution enables teams to map multiple framework requirements to each other, allowing teams to consolidate compliance activities and eliminate redundant controls.

3. **Integrates with existing IT risk and compliance databases**
   The technology's API can integrate with other best-in-breed technologies that may already be part of your ecosystem (ex. Alteryx, Snowflake).

4. **Connects your risk and compliance activities**
   The solution connects your risk and compliance data and activities in a way that reduces duplicate efforts, promotes collaboration, and drives better decision making across the three lines.

5. **Promotes stakeholder accountability**
   The platform helps reduce stakeholder touchpoints and improves stakeholder engagement and accountability.

6. **Intuitive and simple to use**
   The technology's user interface lends itself to an easy, intuitive user experience, also contributing to high adoption rates.

7. **Reduced time to complete audits**
   Streamlined compliance activities lead to significantly reduced time completing audits.

8. **Experienced solution support**
   The technology has an excellent customer support track record, and implementation leads and solution experts with industry expertise.

9. **Reporting features that allow you to quantify risk impacts to executives**
   The solution has configurable dashboards and integrations with data visualization tools that empower you to clearly communicate risk impacts to the business.

10. **Quick implementation time**
    Time to value is not dependent on having the solution completely built out; simply put, product stand-up is quick, effective, and immediately applicable.

In Conclusion

Greater local and federal regulatory scrutiny on insurance organizations' cybersecurity posture is here to stay, and the consequences of ineffective IT risk and compliance have been made abundantly clear. In light of the regulatory developments described above, it is important to consider the reactionary costs of noncompliance — including multimillion dollar penalties and legal costs — may far outweigh the upfront costs of investment in resources to strengthen your IT risk and compliance infrastructure. For insurance organizations seeking to stay ahead of the competition, the rationale for swift, proactive action to strengthen your IT security posture is evident: the time to act is now.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, IT security, and ESG management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fourth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.