Deloitte.

Responding to a Cyber event: ICFR considerations

Internal audit megatrends | 5x5: Insights and actions

Today's Internal Audit & SOX teams manage competing priorities as they work to navigate the growing complexities within the cyber environment. In addition to rapidly growing systems, interconnected regulations, and increased risks—worldwide cybercrime costs are estimated to hit $10.5 trillion annually by 2025[1]. It is no longer a matter of if, but when, an organization is breached. A rapid response from the IT Security team and a coordinated response from the Internal Audit team (IA)* can support management's conclusion on the potential impact to the financial statements and aide in the maintenance of the internal control environment. For organizations looking to be prepared when an event does occur, here are five insights to consider and five actions you can take.

[1] Per the World Economic Forum, "The need for international rules to tackle cybercrime," Published January 2, 2023

5 insights ICFR leaders should know

1. The SEC Rules on **Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure** became effective December 18, 2023, which require public companies to **disclose both material cybersecurity incidents** and, on an annual basis, material information regarding their cybersecurity risk management, strategy, and governance.

2. Accounting implications for cyber events are **complex and unclear** until the event occurs, and digital forensics isolates and analyzes the data compromised, as each attack is unique in scope and extent of the breach.

3. **Accuracy** of and **speed** to concluding on control deficiency(ies) and conclusion of additional control testing and procedures performed by management to validate data recovered (from backup point to time systems went down) and re-entered (data captured between time system went down to the time systems were brought back online and operating business as usual) is crucial to assist external audit in filing an accurate and timely 10Q or 10K.

4. Involving the IA team in war game exercises as well as cyber event preparation and response is crucial in **building trust**, presenting a united front, and **adding value** to the business in preparation of and during a crisis.

5. When examining current and future roles in addressing cyber events, the IA team can help organizations **accelerate recovery, maintain the internal control environment, and support management's response.**

*Management may have various stakeholder which are responsible for the implementation of the ICFR environment.

5 actions IA departments can take

Pre-incident

1. To be strategic, proactive, and add value in preparation of and during a crisis, the IA team should engage in crisis management discussions with management, regarding current cyber trends which emphasize **system hardening standards,** pen test results and remediation actions, and the **existence of manual standard operation procedures (SOPs) in case of system shutdown** so that the business can remain operationally functional during a cyber event.

2. As the External Audit Team will need to be engaged regarding ICFR assessments and conclusions related to a cyber breach, the IA team should **have strategic planning discussions with the External Audit team** regarding **the point of contact, methods for communication, and expected response protocol(s)** if a breach were to occur as this will maximize speed to resolution and conclusions. This should include a consideration and discussion as to whether the ICFR risk assessment (including Financial Statement Line Item (FSLI) assessment template) considers a potential cyber breach.

During incident

3. **Engage in key meetings** with legal, External Audit, IT security, and the business through incident containment and recovery to support the business in **documenting internal controls** and management's **analysis of the control deficiency**. During internal meetings with the business, provide perspective of important audit considerations to guide management's response procedures.

Post-incident

4. Leveraging the FSLI assessment template and knowledge gained during key stakeholder meetings, **perform an exposure check** to identify FSLIs which were impacted during the incident and had a high volume of transactions during the "down time." **Triage the FSLIs** by assessing the downtime procedures executed, data catch up procedures followed, compensating controls, and volume and materiality of data transacted.

5. **Evaluation of the impact** should consider four key elements**:**
   - **Impact on financially relevant processes** by testing management's processes for **data cut-off** and **manual transaction catch-up.** Determine the scope of what could have gone wrong, by comparing compromised accounts to accounts with access to financially relevant systems and systems accessed by the threat actor.
   - Document what **controls were set up or relied upon** during the outage.
   - **Analyze compensating controls** that mitigated the risk of material misstatement.
   - Deliver **advice and recommendations**, including root cause analysis, areas of improvement, and remediation plans. Support management in the preparation of the **deficiency memo.**

Internal audit – Ways to engage:

Participate in war game exercises to assess the effectiveness of manual ICFR control activities and identify areas of improvement.

Perform a risk assessment of FSLIs to inform cyber response approach and expedite analysis of impact through capturing volume and materiality of data transacted in each FSLI.

Evaluate event impact on the financial statements through testing of management's consideration of data cut-off point and processes for manual transaction catch-up. Analyze compensating controls that mitigated the risk of material misstatement.

Review manual SOPs for both IT and business process and provide recommendations on documentation to retain in order to maintain the control environment and enable testing by internal and external audit.

Assist in risk assessment and scoping considerations dependent on the nature, extent, and type of breach, as well as performance of analytics to identify abnormal manual activities or account balance fluctuations.

Evaluate / align ERM focus areas with the IT & SOX risk assessment to inform cyber response approach and determine whether the business is able to meet operational and regulatory requirements.

This publication contains general information only and Deloitte Risk & Financial Advisory is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte Risk & Financial Advisory shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

For more information, or to explore insights visit:
Internal Audit: Risks and Opportunities

Contact us:

Sarah Fedele
Internal Audit Managing Principal
Deloitte & Touche LLP
sarahfedele@deloitte.com

Pete Low
Advisory Managing Director
Deloitte & Touche LLP
plow@deloitte.com

Vipul Patel
Advisory Managing Director
Deloitte & Touche LLP
vbpatel@deloitte.com

Geoffrey Kovesdy
Advisory Principal
Deloitte & Touche LLP
gkovesdy@deloitte.com

Morgan Kroeger
Advisory Manager
Deloitte & Touche LLP
mkroeger@deloitte.com