AUDITBOARD

Top 5 Operational Audits For a Well-Rounded Audit Plan

A successful audit team is one that not only meets its SOX requirements, but can prove itself a valuable partner to the business by identifying key areas for improving operational efficiency. For auditors, this begins with the audit plan. A well-rounded audit plan will reflect an enterprise-wide scope and coverage of risks while addressing audit projects focused on improving operational performance across the business. This brief will discuss 5 important internal audits to consider including in your audit plan.

1. CYBERSECURITY

The continued rise of cyber attacks, which occur extremely quickly and cause critical damage in little time, points to the importance of building cyber resiliency. Internal audit can help by auditing and evaluating measures that prevent an attack and also mitigate risk in the event of one.

Cyber Crime Statistics in 2019:

87%	**$6T**	**56%**
cyber attacks in 1 min or less	cybercrime damages	experienced vendor breaches

- 87% of cyber attacks occurred in minutes or less, but 68% of breaches took months or longer to discover [1]
- Cybercrime damages are predicted to exceed *$6 trillion* by 2021
- 56% of organizations have experienced a breach caused by a vendor [2]

**Educate yourself on the biggest threats to your industry - review the Verizon DBIR summary*

Recommended Audit Projects:

- **Data Encryption.** Ensure that data classification policies exist to identify and appropriately classify confidential data. Data classified as confidential or sensitive in nature should be encrypted in transit and at rest.

- **Access Management Policies and Controls.** Review access rights are granted based on properly-defined business needs and evaluate the timing of access rights termination when employees leave the organization.
- **Data Penetration Testing with Vendors.** Ensure your third-party vendors and contractors maintain and execute information security policies and controls that meet or exceed internal requirements.
- **Business Continuity Plan (BCP).** Audit the overall business continuity plan to ensure that appropriate considerations are in place for maintaining core business functions in the event of an infrastructure failure, cybersecurity incident, natural disaster, or other emergencies. Confirm if the business is performing routine BCP tabletop exercises, updating contacts and procedures on a regular basis, and distributing the BCP to all relevant parties.
- **Patch Management Policies.** Audit whether patch and vulnerability management policies are in place to ensure that patches are implemented in a timely fashion upon release and testing.
- **Employee Information Security Training.** Evaluate employee security training materials and effectiveness of training programs. Every single employee in an organization should receive and sign off on information security training materials. Training and policies should be updated on a regular basis (annually at a minimum). [3]

2. CULTURE AND ETHICS

Companies are facing more cultural accountability today than ever before. Unprecedented reputational risks are casting looming shadows over shareholder confidence, thanks to the rise of the #MeToo movement in response to sexual harassment in the workplace and growing public concern over consumer data privacy. Internal Audit can help mitigate future reputational risks by promoting appropriate workplace ethics and values.

Recommended Audit Projects:

- **Digital Ethics.** Evaluate how consumer information is managed and protected across the enterprise, including within departments such as marketing and sales. Identify whether ethics goals are included as a part of performance metrics and annual performance reviews.
- **Succession Planning.** Review succession planning methodology for whether the company has adequate talent retention procedures or policies. Encourage the use of cross-department trainings and hiring collaboration.
- **Gender and Racial Discrimination.** Evaluate hiring, pay, and promotion review procedures across the organization's departments. Identify potential external areas of concern, such as employee-customer touchpoints, and evaluate employee and customer feedback. Build comparison groups from this information gathering to identify deviations in response across gender and racial demographics, highlighting potential bias.

3. DATA PRIVACY

Corporate mishandling of consumer data has become a topic of national security and poses a huge reputational risk to companies. The Facebook-Cambridge Analytica scandal and Google's $57 million GDPR fine are two notoriously publicized examples, but organizations of all sizes and industries have experienced severe data breaches resulting in damaged public opinion of those brands.[4] Internal audit should understand how personal information is being stored and managed and ensure there are proper security controls in place.

Recommended Audit Projects:

- **General Data Protection Regulation (GDPR) Enforcement.** If your organization serves any citizens within the European Union (EU), it is within the scope of GDPR enforcement. Perform a GDPR audit to identify all data processing objects and activities, including those stored or controlled by third party businesses or vendors. To identify whether your organization's handling of data in scope for GDPR is appropriate, consider engaging external firms or contractors who specialize in GDPR-readiness.
- **Consumer Consent.** Audit your company's compliance with consumer privacy regulations and review privacy consent policies and effectiveness across departments. Ensure that pseudonymization is in place to remove personalized identifiers. [5]

4. DATA GOVERNANCE

In contrast to consumer data, big data refers to organizational data, which is unstructured and housed in different silos. Understanding and incorporating big data into strategic business decisions poses new challenges and risks, namely data accountability and protection. Internal Audit can help ensure proper data governance controls and policies are in place.

Recommended Audit Projects:

- **Data Quality.** Areas to audit: data migration procedures, data management procedures in the event of acquisitions, data quality standards.
- **Data Analytics.** Areas to audit: policies and procedures of data analytics functions, proper storage and ownership controls around data repositories and self-service platforms, data access controls.

5. THIRD PARTY RISK

External talent, data centers, and vendors help businesses promote productivity and efficiency, but they come at the cost of incurring complex third party risks. Over two-thirds of organizations using vendors have reported fines, lost revenues, or brand damage caused by third parties. Internal audit can identify control weaknesses and recommend improvements regarding third party risk.

Recommended Audit Projects:

- **Background Checks.** One of the most basic but effective controls is ensuring third party contractors undergo and pass background checks that meet or exceed internal requirements prior to the contract start date.
- **Third Party Risk Management.** Evaluate the organization's third party risk management framework from end to end, ensuring that vendor risk is appraised across all functional areas of the business, and that risk assessments and mitigation activities are performed on a routine basis.
- **Contract Management.** Evaluate contract management processes used to track relationships with vendors. Ensure that vendor relationships are evaluated regularly and that legacy contracts include required clauses.
- **Right-to-audit Clauses.** Ensure possible rights to audit are included in all contracts and perform periodic reviews and updates
- **Monitoring and Compliance.** Assess third party compliance by developing, implementing, and performing monitoring around a compliance system that is aligned with the company's information security standards.

To learn how OpsAudit can help you manage your internal audit projects - request a product walkthrough at *auditboard.com*.

---

[1] Verizon, 2018 Data Breach Investigations Report (*https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf*)

[2] Gartner, 2019 Audit Hot Spots Report Excerpt (*https://emtemp.gcom.cloud/ngw/globalassets/en/risk-audit/documents/audit-hot-spots.pdf*)

[3] Isaca, Auditing Cyber Security: Evaluating Risk and Auditing Controls (*http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/auditing-cyber-security.aspx*)

[4] Gartner, 2019 Audit Hot Spots Report Excerpt (*https://emtemp.gcom.cloud/ngw/globalassets/en/risk-audit/documents/audit-hot-spots.pdf*)

[5] International Association of Privacy Professionals, Top 10 Operational Impacts of the GDPR - Part 8: Pseudonymization (*https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/*)

[6] KPMG, Top 10 Audit Concerns 2018 (*https://advisory.kpmg.us/content/dam/advisory/en/pdfs/top10auditconcerns-2018.pdf*)

Copyright © 2019 AuditBoard Inc.