# 2016 Audit Plan Hot Spots

## Top 5 Preview Report

CEB Audit Leadership Council

CEB
WHAT THE BEST COMPANIES DO

# Objective

Our Audit Plan Hot Spots series identifies and analyzes emerging risk areas that internal audit departments anticipate focusing on during the next 6–12 months. Our hot spots research enables audit directors to do the following:

- **Benchmark Audit Plan Coverage—**Compare, validate, and further examine audit plan coverage.
- **Audit Committee Education—**Educate the audit committee on risk trends that impact global organizations.
- **Audit Team Discussions—**Create a platform for audit engagement planning and scoping.
- **Emerging Risk Sensing—**Use the collection of key risk indicators to uncover areas of increasing risk exposure.
- **Risk Assessment—**Ask these questions to prepare management for risk assessment or audit scoping discussions.

In this year's full report, each Hot Spot has two pages. The first page outlines the nature of the risk, its drivers, and Audit's role. The second page provides practical support for auditing the risk (e.g., questions for Audit to pose to management).

# Top 5 Hot Spots Summary

| Audit Plan Risk Areas | Risk Drivers |
|---|---|
| **1. Data Privacy**<br>Detailed in this preview. | The recent string of high-profile data breaches has put the risks surrounding data privacy squarely top of mind this year. Companies are rapidly digitalizing their operations but are not updating associated governance measures at the same pace, and employee training on privacy regulations fails to drive more risk-aware behavior. The costs of poor data privacy are mounting—in addition to regulatory noncompliance, companies face large costs in terms of management time and lost business. |
| **2. Cybersecurity** | The number of cybersecurity incidents increased by 48% over the last year. Cybersecurity is a board-level issue and remains a critical risk, as the increased attention has not yet been translated into adequate detection and response measures across organizations. Even as organizations shore up their external defenses, they remain vulnerable to attacks from malicious insiders (employees and third-party contractors), which are harder to prevent and potentially more damaging. |
| **3. Third-Party Relationships** | Organizations continue to create an increasing number of third-party relationships—the median company now has 3,000. Third parties are also taking on increasingly critical business functions. Despite this, organizational oversight remains limited. Attaining proper oversight is complicated by the ongoing decentralization of procurement activities, driven by the increasing speed of business. This lack of oversight leaves organizations exposed to significant risk in terms of business disruptions, data leaks, and regulatory noncompliance. |
| **4. Strategic Change Management**<br>Detailed in this preview. | To meet aggressive growth targets, organizations are implementing more and more strategic change initiatives. However, the combined speed, frequency, and volume of these initiatives can often lead to failure in execution. These change initiatives also risk degrading the control environment by causing change fatigue in employees: risk management effectiveness declines on average by 6% in areas affected by material change. |
| **5. Business Continuity and Disaster Recovery** | The relentless geographic expansion of companies' operations and supply chains, coupled with a focus on lean operations and single sourcing, has increased companies' exposure to unforeseeable risk events that could cause business disruptions. As the number and type of risks continue to grow, companies' ability to properly respond to adverse events has been further complicated by an increasing difficulty in insuring against new or immeasurable risks. |

**Contact us to learn about the remaining five Audit Hot Spots and dive deeper into the full report.**

**Email: Audit.Support@cebglobal.com Phone: +1-866-913-8103 Web: cebglobal.com/audit**

# Data Privacy

High-profile data breaches at Sony Entertainment, JP Morgan, and Premera show that no industry is safe from this risk. Consequences of privacy failures can be far-reaching and expensive: lost business, regulatory noncompliance, and the cost of management time. These indirect costs can be 10 times larger than the costs of the initial response to the breach itself.[6] In 2016, regulatory action is poised to become increasingly painful; in the United States, the FCC recently levied a record $25 million fine, and Europe may pass a law allowing fines of up to 5% of an organization's global revenue. Despite the increasing risks, only 30% of privacy officers are satisfied with their privacy program, and 72% of companies audit privacy controls less than annually or not at all.[7]

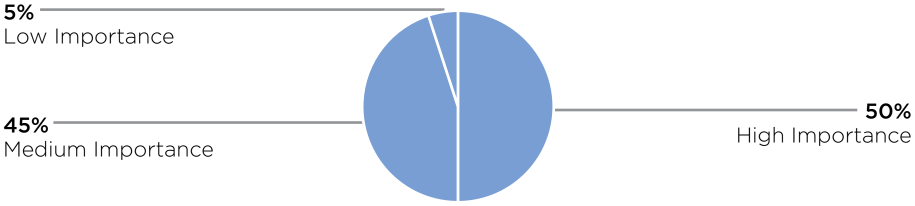
1. **Dependence on Digitalization:** Today, competition propels almost every organization to embrace data-driven capabilities, from big data to mobile devices, as a key component of corporate strategy. For example, manufacturers now connect their products to the Internet of Things, while utilities deploy automated meters to analyze usage data. These data-driven strategies process large volumes of information, which strains outdated governance and controls. Although eager to digitalize business models, many companies are unprepared for the associated risks. Forty-two percent of companies do not have an accurate inventory of where data is collected, transmitted, and stored, and almost 50% of privacy officers state that operational complexity prevents them from building an effective privacy program.[8,9]
2. **Overreliance on Technical Controls:** As concern about data breaches intensifies, companies attempt to address this risk with technical solutions.[10] However, effective prevention requires well-trained employees: 70% of IT practitioners report that more incidents are caused by unintentional mistakes than by malicious acts.[11] Despite the significant role employee behavior plays, privacy resources are not proportional to those dedicated to technical controls. The average information security budget is 14 times larger than the average privacy budget, and the median company only provides employees with an hour of annual privacy training.[12,13] As a result, employees are often unaware of data privacy risks and requirements or of the purpose of related controls.

## Role of Internal Audit

Audit should review the processes related to the collection, analysis, storage, and sharing of personal information and ensure the appropriate controls are integrated into all projects and initiatives. Audit should test the efficacy of privacy training and awareness campaigns, ensuring they drive appropriate improvements in employee awareness and behaviors regarding privacy risks.

Importance of Providing Assurance Over Data Privacy Risk

*Percentage of Respondents*

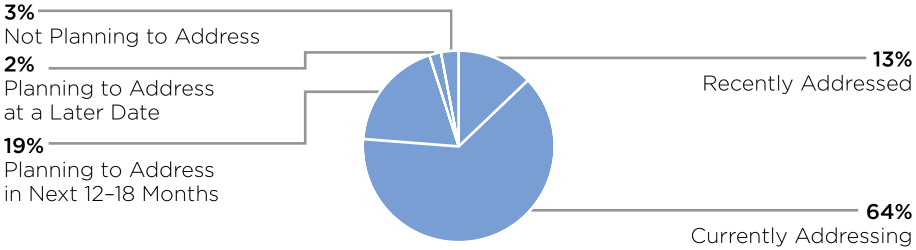


*n* = 108.

Source: CEB 2016 Agenda Setting and Hot Spots Survey.

Status of Providing Assurance Over Data Privacy Risk

*Percentage of Respondents*



*n* = 108.

Source: CEB 2016 Agenda Setting and Hot Spots Survey.

Note: Pie does not total 100% due to rounding.

# Data Privacy: Audit Support

*Sample Detail Summary*

## 2016 Audit Plan Additions

- **Personal Information Mapping Review:** Ensure the effectiveness of information governance by certifying the business has classified, inventoried, and mapped all personal information stored by the organization. Verify that each data type has an owner responsible for monitoring access and for approving any requests to share the data with third parties.
- **Information Governance Assessment:** Confirm the organization has identified a single individual to coordinate management of privacy risks. Ensure that Privacy and Information Security have clearly delineated roles and responsibilities and that no gaps or redundancies exist.
- **Employee Behaviors Test:** Assess whether training initiatives effectively drive privacy-aware employee behavior. Check whether training targets high-risk employee populations and whether it enables employees to translate privacy concepts to their specific workflows.

## Business Value at Stake

Effective privacy governance and controls facilitate easy access to personal data while enhancing customer trust. Companies that commit to better data governance will be able to analyze more higher-quality personal information than their competitors. Overall, using data to better inform business decisions can create enormous strategic advantages for organizations by enhancing their ability to anticipate customer needs and broader consumer trends and to customize products to user desires.

## Questions to Management

- Does your function or division currently oversee specific processes that transfer or use significant amounts of personal information? How do you secure that information?
- How do you assess the benefits of data collection against the potential risks to prevent gratuitous collection of data?
- What types of communication (e.g., training, awareness materials) do you use to communicate privacy risks and policies to employees?
- How do you measure the efficacy of data privacy training?
- Which regimes govern your use of PII? What changes in these regulations do you anticipate in the next year, and how are you preparing for those changes?

## Key Risk Indicators

- Number of reports of privacy violations and the percentage substantiated
- Number of downloads of the company privacy policy
- Number of employees who can access sensitive PII (Personally Identifiable Information)
- Number of new or proposed privacy laws that will impact the company
- Number of third parties with which PII is shared
- Percentage of employees who complete privacy training
- Type and volume of PII data attributes on our network

## CEB Audit Resources

- Data Privacy Risk Resource Center
- Data Privacy Program Archetypes
- Build and Measure a Security-Focused Mind-Set in Employees
- Data Privacy Awareness Questionnaire
- Privacy Impact Assessment
- Data Privacy Audit Program
- Business Case for a Data Privacy Function

# Strategic Change Management

Executives face aggressive growth and cost-cutting targets. Sixty-seven percent of business leaders expect revenue targets to increase, while 67% expect cost pressures to increase.[28] To meet these objectives, companies are putting renewed efforts into strategic change initiatives, including organizational restructuring, new technology systems, geographic expansion, and new product development. Material changes in an organization negatively impact the effectiveness of risk management, which declines, on average, by 6%.[29] Trends of relevance to Audit this year include:

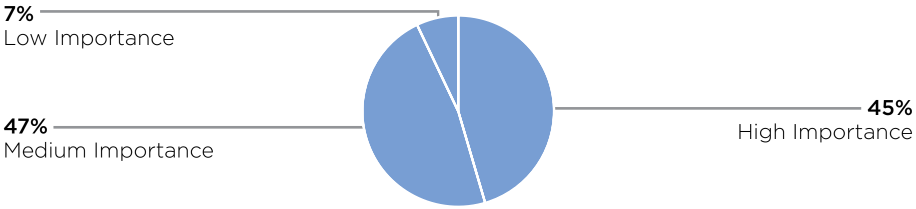
1. **Frequent Change Leading to Strategy Execution Failure:** The speed and frequency of changes are increasing. Companies' large cash reserves, coupled with low borrowing costs, have led to an increase in mergers and acquisitions.[30,31] Eighty-two percent of surveyed executives are planning at least one acquisition in 2015, while 10% are planning 11 or more deals.[32] In addition, companies have seen significant changes in their leadership, processes, or staffing models.[33] Audit teams report having observed, on average, six such material changes at their organizations during the last year.[34] However, the simultaneity and volume of these changes is impairing the ability of employees to successfully support business objectives.[35] Only 21% of the workforce is actively aligning their efforts to strategic goals,[36] causing strategy execution to suffer—which results in more than one in three strategic initiatives failing.[37]
2. **Employee Fatigue Resulting from Frequent Change:** Frequent instances of strategic change lead to "change fatigue"—when employees experience greater levels of cynicism and exhaustion. Almost 65% of employees at all levels indicated experiencing change fatigue in some form in a recent survey.[38] Control owners—employees who determine, maintain, or direct policies and procedures—feel this fatigue most acutely. Change fatigue among this group results in higher levels of disengagement and turnover, as well as greater levels of control deficiencies,[39] putting stress on the risk management environment.

## Role of Internal Audit

Audit should ensure a rigorous risk assessment process is followed for all change initiatives and that communication, staff resources, and capacity all contribute to effective strategy execution. Audit should review the integrity of the control environment during change initiatives and scrutinize gaps in affected control systems.

Importance of Providing Assurance Over Strategic Change Management Risk

*Percentage of Respondents*



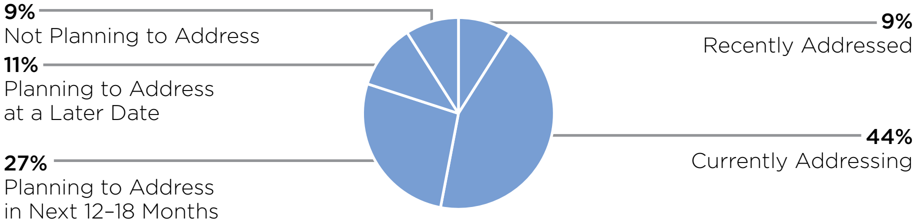
*n* = 108.

Source: CEB 2016 Agenda Setting and Hot Spots Survey.

Note: Pie does not total 100% due to rounding.

Status of Providing Assurance Over Strategic Change Management Risk

*Percentage of Respondents*



*n* = 108.

Source: CEB 2016 Agenda Setting and Hot Spots Survey.

# Strategic Change Management: Audit Support *Sample Detail Summary*

## 2016 Audit Plan Additions

- **Basic Operating Controls Review:** Review the process for identifying and ensuring the effectiveness of basic operating controls. Test whether this process is conducted in a timely and comprehensive manner to help spot control gaps and weaknesses as the organization implements change initiatives.
- **Strategy Communication and Awareness Audit:** Review the process of communicating strategic change initiatives to all levels of the organization, and evaluate the level of understanding of corporate strategy and alignment with day-to-day work at different levels of responsibility.
- **Employee Engagement Review:** Assess management's practices of identifying and responding to signs of employee disengagement, ensuring they use regular conversations to evaluate engagement, and note changes in attitude and behaviors. In addition, ensure these results are documented and that action plans exist to address signs of employee disengagement.

## Business Value at Stake

By ensuring effective strategic change management and communication, organizations can ensure that employees understand and contribute to the achievement of strategic goals. Reacting to changes in the corporate environment is inevitable in today's world, and an organization that quickly recovers from change will gain a large competitive advantage over their peers.

## Questions to Management

- How do you assess the potential impact of strategic change initiatives on your business environment?
- How do you ensure the comprehensiveness of your due diligence process before deciding to merge with or acquire a company?
- How do you assess your employees' motivation and engagement levels, especially for employees responsible for managing risks?
- What are the expected implications of change initiatives on your organization's business operations?
- What is your risk assessment process to determine the feasibility of strategic change initiatives?
- How do you determine if and when a project should be terminated?

## Key Risk Indicators

- Existence of documented risk assessment reviews for all strategic change initiatives
- Level of employee engagement scores in business areas experiencing change
- Level of employee turnover in business areas impacted by change
- Employee productivity levels in business areas undergoing change
- Percentage of projects experiencing cost overruns
- Percentage of projects delayed
- Ratio of failed projects to projects undertaken

## CEB Audit Resources

- Strategy and Growth Project Risk Resource Center
- Signs of Employee Disengagement
- Project Health Checks
- Strategic Planning Assurance Checklist
- Project Management Audit Program
- Strategic Risk Management Audit Program
- M&A Due Diligence Audit Program
- M&A Integration Audit Program