# 2015 Audit Plan Hot Spots

## Top 5 Preview Report

### Objective

CEB's Audit Plan Hot Spots series identifies and analyzes emerging risk areas that internal audit departments anticipate focusing on across the next 6 to 12 months, enabling audit directors to do the following:

- Spot risk trends and interdependencies
- Highlight emerging risk areas
- Benchmark audit plan coverage
- Inform audit committee discussions

CEB Audit Leadership Council

CEB
WHAT THE BEST COMPANIES DO

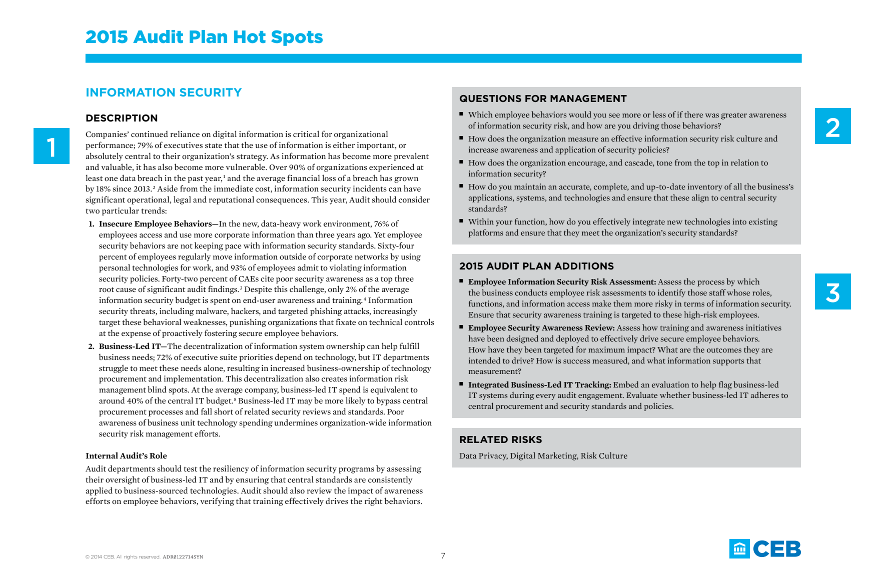
# 2015 Audit Plan Hot Spots

## INTRODUCTION TO HOT SPOTS

### HOW TO USE HOT SPOTS

- **Benchmark Audit Plan Coverage:** Use the hot spots research to compare, validate, and/or further examine audit plan coverage.
- **Audit Committee Education:** Use the hot spots research to educate the audit committee on the risk trends impacting global organizations.
- **Audit Team Discussions:** Use the hot spots research as a platform for audit engagement planning and scoping.
- **Emerging Risk Sensing:** Use the collection of key risk indicators to surface areas of increasing risk exposure.
- **Risk Assessment:** Use the questions to prepare management for risk assessment or audit scoping discussions.

### HOW TO READ HOT SPOTS



2015 Audit Plan Hot Spots

INFORMATION SECURITY

DESCRIPTION

Companies' continued reliance on digital information is critical for organizational performance; 79% of executives state that the use of information is either important, or absolutely central to their organization's strategy. As information has become more prevalent and valuable, it has also become more vulnerable. Over 90% of organizations experienced at least one data breach in the past year,[1] and the average financial loss of a breach has grown by 18% since 2013.[2] Aside from the immediate cost, information security incidents can have significant operational, legal and reputational consequences. This year, Audit should consider two particular trends:

1. **Insecure Employee Behaviors**—In the new, data-heavy work environment, 76% of employees access and use more corporate information than three years ago. Yet employee security behaviors are not keeping pace with information security standards. Sixty-four percent of employees regularly move information outside of corporate networks by using personal technologies for work, and 93% of employees admit to violating information security policies. Forty-two percent of CAEs cite poor security awareness as a top three root cause of significant audit findings.[3] Despite this challenge, only 2% of the average information security budget is spent on end-user awareness and training.[4] Information security threats, including malware, hackers, and targeted phishing attacks, increasingly target these behavioral weaknesses, punishing organizations that fixate on technical controls at the expense of proactively fostering secure employee behaviors.
2. **Business-Led IT**—The decentralization of information system ownership can help fulfill business needs; 72% of executive suite priorities depend on technology, but IT departments struggle to meet these needs alone, resulting in increased business-ownership of technology procurement and implementation. This decentralization also creates information risk management blind spots. At the average company, business-led IT spend is equivalent to around 40% of the central IT budget.[5] Business-led IT may be more likely to bypass central procurement processes and fall short of related security reviews and standards. Poor awareness of business unit technology spending undermines organization-wide information security risk management efforts.

**Internal Audit's Role**

Audit departments should test the resiliency of information security programs by assessing their oversight of business-led IT and by ensuring that central standards are consistently applied to business-sourced technologies. Audit should also review the impact of awareness efforts on employee behaviors, verifying that training effectively drives the right behaviors.

QUESTIONS FOR MANAGEMENT

- Which employee behaviors would you see more or less of if there was greater awareness of information security risk, and how are you driving those behaviors?
- How does the organization measure an effective information security risk culture and increase awareness and application of security policies?
- How does the organization encourage, and cascade, tone from the top in relation to information security?
- How do you maintain an accurate, complete, and up-to-date inventory of all the business's applications, systems, and technologies and ensure that these align to central security standards?
- Within your function, how do you effectively integrate new technologies into existing platforms and ensure that they meet the organization's security standards?

2015 AUDIT PLAN ADDITIONS

- **Employee Information Security Risk Assessment:** Assess the process by which the business conducts employee risk assessments to identify those staff whose roles, functions, and information access make them more risky in terms of information security. Ensure that security awareness training is targeted to these high-risk employees.
- **Employee Security Awareness Review:** Assess how training and awareness initiatives have been designed and deployed to effectively drive secure employee behaviors. How have they been targeted for maximum impact? What are the outcomes they are intended to drive? How is success measured, and what information supports that measurement?
- **Integrated Business-Led IT Tracking:** Embed an evaluation to help flag business-led IT systems during every audit engagement. Evaluate whether business-led IT adheres to central procurement and security standards and policies.

RELATED RISKS

Data Privacy, Digital Marketing, Risk Culture

© 2014 CEB. All rights reserved. ADRØ122714SYN 7

CEB

1 Understand why a particular issue matters to businesses today.

2 Identify key questions for each issue.

3 Integrate specific audits into your current or future audit plans.

# 2015 Audit Plan Hot Spots

## TOP 5 HOT SPOTS SUMMARY

| Audit Plan Risk Areas | Risk Drivers |
|---|---|
| **Information Security** | Organizations' increased reliance on digital information has dramatically increased the vulnerability of their networks and systems. Insecure employee behaviors and the decentralization of information system ownership have exacerbated this risk, with 93% of employees admitting to violating information security policies and with an increase in business-led IT spend to 40% of the central IT budget. |
| **Strategic Change Management** | To improve profitability, 80% of CEOs report either being actively involved in, or strongly considering, a strategic transformation of their organizations. However, companies are increasingly finding themselves without sufficient resources required to successfully execute these strategic initiatives. Poorly conducted organizational changes also expose companies to the risk of obsolete control environments. |
| **Climate Change and Extreme Weather Events** | Extreme weather events caused over $120 billion of loss to local economies in 2013, impacting companies' operating costs, performance, and ability to do business. Heightened regulatory requirements have also forced organizations to rethink how they produce and distribute goods, and how they demonstrate commitment to sustainability through their activities. |
| **Geopolitical Instability** | More than 70% of CEOs surveyed have expressed concerns about geopolitical tensions and their impact on growth prospects. Intensifying political instability in many parts of the world has a material impact on operational continuity in affected markets and is likely to cut off current and prospective customers. Beyond political instability, uncertainty about policy making and reform and governmental activity is also driving this risk, as there is greater uncertainty about how operations may be impacted, which may cause firms to postpone their investments. |
| **Data Privacy** | Increased collection, analysis, and storage of customer and employee information has magnified companies' exposure to compliance and reputational risks. The proliferation and decentralization of data makes material data breaches almost impossible to prevent or detect. The rapid growth of regulations challenges the effective governance of data privacy at companies, creating compliance difficulties. |

**Contact us at LRCProductMarketing@executiveboard.com to learn about the remaining five Audit Hot Spots.**

## INFORMATION SECURITY

### DESCRIPTION

Companies' continued reliance on digital information is critical for organizational performance; 79% of executives state that the use of information is either important, or absolutely central to their organization's strategy. As information has become more prevalent and valuable, it has also become more vulnerable. Over 90% of organizations experienced at least one data breach in the past year,[1] and the average financial loss of a breach has grown by 18% since 2013.[2] Aside from the immediate cost, information security incidents can have significant operational, legal and reputational consequences. This year, Audit should consider two particular trends:

1. **Insecure Employee Behaviors**—In the new, data-heavy work environment, 76% of employees access and use more corporate information than three years ago. Yet employee security behaviors are not keeping pace with information security standards. Sixty-four percent of employees regularly move information outside of corporate networks by using personal technologies for work, and 93% of employees admit to violating information security policies. Forty-two percent of CAEs cite poor security awareness as a top three root cause of significant audit findings.[3] Despite this challenge, only 2% of the average information security budget is spent on end-user awareness and training.[4] Information security threats, including malware, hackers, and targeted phishing attacks, increasingly target these behavioral weaknesses, punishing organizations that fixate on technical controls at the expense of proactively fostering secure employee behaviors.
2. **Business-Led IT**—The decentralization of information system ownership can help fulfill business needs; 72% of executive suite priorities depend on technology, but IT departments struggle to meet these needs alone, resulting in increased business-ownership of technology procurement and implementation. This decentralization also creates information risk management blind spots. At the average company, business-led IT spend is equivalent to around 40% of the central IT budget.[5] Business-led IT may be more likely to bypass central procurement processes and fall short of related security reviews and standards. Poor awareness of business unit technology spending undermines organization-wide information security risk management efforts.

### Internal Audit's Role

Audit departments should test the resiliency of information security programs by assessing their oversight of business-led IT and by ensuring that central standards are consistently applied to business-sourced technologies. Audit should also review the impact of awareness efforts on employee behaviors, verifying that training effectively drives the right behaviors.

### QUESTIONS FOR MANAGEMENT

- Which employee behaviors would you see more or less of if there was greater awareness of information security risk, and how are you driving those behaviors?
- How does the organization measure an effective information security risk culture and increase awareness and application of security policies?
- How does the organization encourage, and cascade, tone from the top in relation to information security?
- How do you maintain an accurate, complete, and up-to-date inventory of all the business's applications, systems, and technologies and ensure that these align to central security standards?
- Within your function, how do you effectively integrate new technologies into existing platforms and ensure that they meet the organization's security standards?

### 2015 AUDIT PLAN ADDITIONS

- **Employee Information Security Risk Assessment:** Assess the process by which the business conducts employee risk assessments to identify those staff whose roles, functions, and information access make them more risky in terms of information security. Ensure that security awareness training is targeted to these high-risk employees.
- **Employee Security Awareness Review:** Assess how training and awareness initiatives have been designed and deployed to effectively drive secure employee behaviors. How have they been targeted for maximum impact? What are the outcomes they are intended to drive? How is success measured, and what information supports that measurement?
- **Integrated Business-Led IT Tracking:** Embed an evaluation to help flag business-led IT systems during every audit engagement. Evaluate whether business-led IT adheres to central procurement and security standards and policies.

### RELATED RISKS

Data Privacy, Digital Marketing, Risk Culture

CEB

## DATA PRIVACY

### DESCRIPTION

As the impact and frequency of material data breaches continue to mount, the controls protecting personal information are not keeping pace: last year, almost half of audit departments reported at least one significant audit finding related to data privacy and protection.[24] Collection and analysis of customer and employee information presents new opportunities but also amplifies compliance and reputational risks. The interconnections between legal, compliance, and IT security risks make it difficult to effectively audit privacy. More than 30% of audit departments do not audit their privacy program at all.[25] In 2015, Audit should consider two trends:

- **Proliferation and Decentralization of Data**—The volume of data has increased 10-fold in the past five years, while the cost of storage has fallen drastically, enabling organizations to accumulate vast stores of data.[26] Equally, the spread of mobile technologies that allow employees to store and access information outside of organizational networks is accelerating. The majority of professionals regularly use personal devices to get work done.[27] These trends contribute to an expanding list of data assets, owners, and users for companies to monitor. However, oversight efforts are often insufficient. Two-thirds of data breaches go undetected for at least three months, demonstrating that current monitoring and detection efforts are ineffective.[28]
- **Heightened Global Regulatory Expectations**—Reflecting the volume, value, and vulnerability of personal information, data privacy regulations are evolving. Organizations are now expected to meet strict and varied standards on the collection, storage, use, and protection of personal information. Cross-border flows of information subject organizations to multiple regulations. Singapore's recent data privacy protections, the EU plans to strengthen data protection rules in 2015, and the various legislation regarding data breaches from most of the United States illustrate the complexity of this environment.[29] The rapid growth of data privacy regulation has challenged the effective internal governance of data privacy. Accountability for data privacy activities, such as interpretation and application of standards, spans multiple functions, complicating compliance efforts. Almost 50% of privacy officers rate the complexity of business operations among the top challenges to building an effective privacy program.[30]

### Internal Audit's Role

Audit should verify that a process is in place to track and interpret regulations and to ensure standards are consistently applied across the organization. It should also establish clear ownership of key data privacy activities. Audit should review processes related to the collection, storage, and transfer of personal information, ensuring that evolving compliance standards have been embedded. Audit should test response plans that are in place to deal with data breaches.

### QUESTIONS FOR MANAGEMENT

- What data that your business currently collects, stores, or uses is subject to data privacy regulations?
- How do you currently ensure the security of that information? How do you set and monitor access controls?
- What processes do you have in place to destroy unnecessary or outdated data?
- How do you monitor regulatory requirements for any over-the-horizon changes that may impact the organization? How frequently do you update the inventory of relevant data privacy regulations?
- When there are multiple regulatory standards relating to a particular data privacy issue, what steps do you take to determine the most applicable standards?

### 2015 AUDIT PLAN ADDITIONS

- **Data Retention and Destruction Review:** Ensure that data retention policies provide clear guidance on retention schedules for different categories of information, are communicated throughout the business, and are applied consistently across functions.
- **Privacy Governance Audit:** Assess whether effective data privacy governance has been established by testing the communication and collaboration between different parties that have some level of responsibility. Verify that each data type has an owner who is responsible for monitoring access. Ensure clarity on roles and responsibilities and that there are no gaps or redundancies.
- **Regulatory Tracking Review:** Certify that the business maintains and regularly updates an inventory of data privacy regulations for each functional or geographic area. Ensure that, for areas where there are multiple and overlapping regulations, the most stringent protocols are being observed.
- **Mobile Technology Policy Assessment:** Confirm that company policies outline permitted uses of mobile technology and define clear limits on the use and storage of personal information on such technologies.

### RELATED RISKS

Information Security, Compliance Management, Third-Party Management, Risk Culture

# 2015 Audit Plan Hot Spots

## SELECTED HOT SPOTS SUPPORT FROM CEB FOR TOP 5 RISKS

### INFORMATION SECURITY

-IT Security and Risk Management ARC Module

-Information Security Risk Primer

-Assure the Effectiveness of Business-Led IT Oversight

-Audit Information Security Governance

-Assess the Impact of Security Awareness Training on Employee Behavior

-External Network Security Audit Program

### STRATEGIC CHANGE MANAGEMENT

-Project Management Review Audit Program

-Project Management Work Program

-Change Management

-Project Risk Assessment

-Mergers and Acquisitions Integration Checklist

-Evaluate Strategy Execution

### CLIMATE CHANGE AND EXTREME WEATHER EVENTS

-Business Continuity Planning and Disaster Recovery ARC Module

-Disaster Recovery Test Plan

-Risk Scenario Workshops

### GEOPOLITICAL INSTABILITY

-International Operations ARC Module

-Managing Risks in Emerging Markets

-Managing Ethics Risk in Asia

-Audit Site Risk Ranking

### DATA PRIVACY

-Data Privacy ARC Module

-Data Breaches, Investigations, and Regaining Control After a Data Security Incident

-Data Privacy Program

-Compliance Checklist

**Contact us at LRCProductMarketing@executiveboard.com to dive deeper into the complete report and learn more about the tools available to support each Audit Hot Spot.**