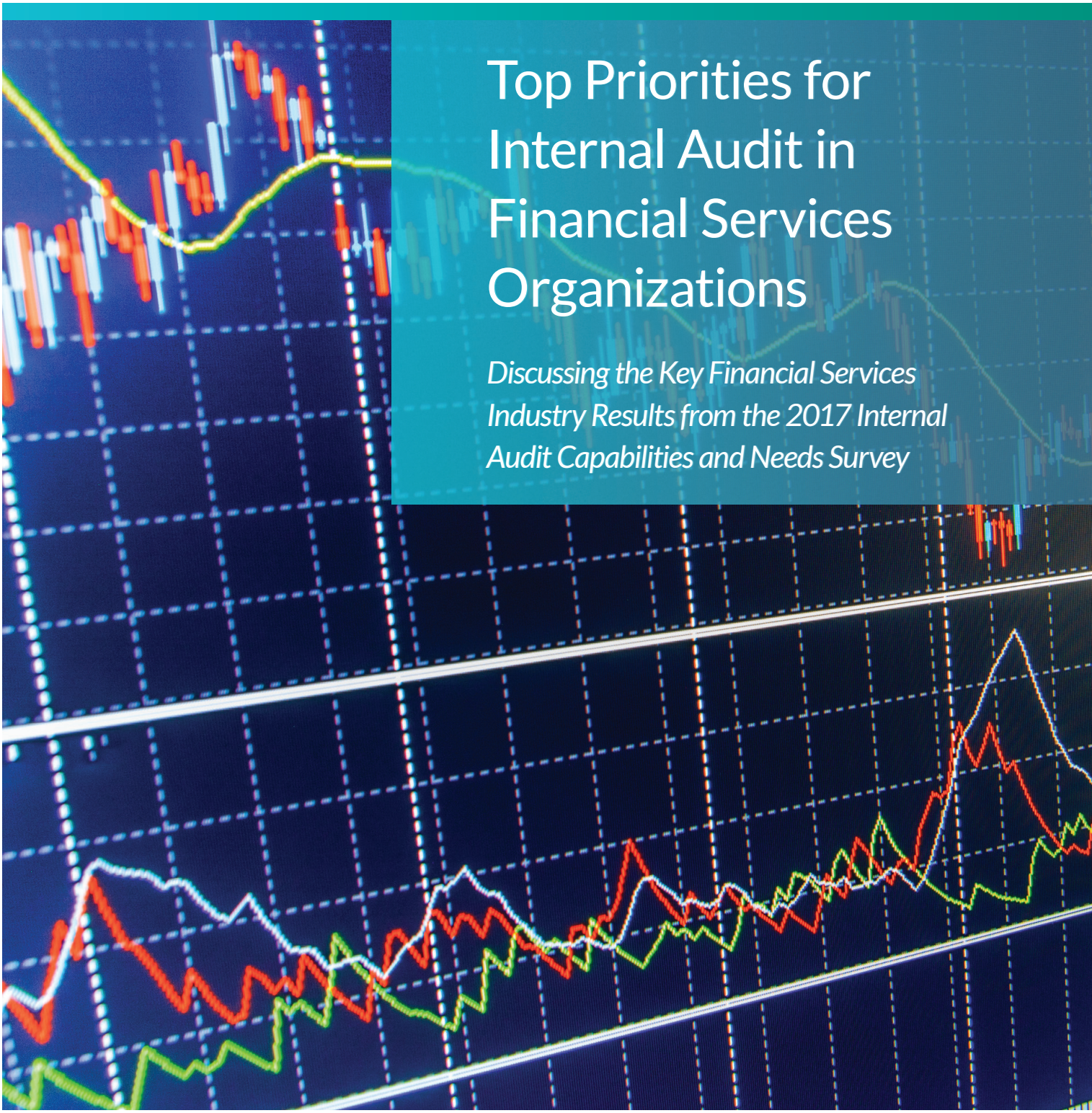
protiviti®

Face the Future with Confidence



Top Priorities for Internal Audit in Financial Services Organizations

Discussing the Key Financial Services Industry Results from the 2017 Internal Audit Capabilities and Needs Survey

Internal Audit, Risk, Business & Technology Consulting

Table of Contents

Introduction

Chief audit executives (CAEs) and their teams are focused on what the future holds for the financial services industry (FSI), which is enduring the return of geopolitical risk and the ever-present challenges of cybersecurity issues, as well as determining their exposure to emerging risks from digital and financial technology companies and services that are changing the economic environment.

Chief executive officers (CEOs), boards of directors and audit committees are increasingly asking CAEs to apply their independent lens and expertise toward analyzing and articulating what the risk future and other emerging risks mean to the organization, its risk profile and the execution of its strategy. CEOs and boards are also asking internal audit functions how increasingly fluid risks within the organization's core risk taxonomy are changing. The frequency and importance of these questions have increased in tandem with growing political, regulatory, economic and technological volatility.

The growing pressure bearing down on internal audit functions is reflected in the FSI findings of Protiviti's annual Internal Audit Capabilities and Needs Survey.[1] The purpose of our survey is to assess current skill levels of internal audit executives and professionals, identify areas being targeted for improvement, and help stimulate the sharing of leading practices throughout the FSI and the internal audit profession. The 2017 findings detailed in the pages that follow capture the outlook of internal audit leaders within the industry. The findings discussed in our paper are based on responses from nearly 200 CAEs and internal audit professionals in the U.S. financial services industry.

This year's respondents identified a number of especially serious challenges related to technology, including:

- Cybersecurity
- Cloud computing
- Big data/business intelligence
- Smart devices, mobile applications and digital transformation.

Yet, technology-related risks are far from the only concern at the very top of internal audit's 2017 priority list. Our respondents also held up the following areas as top areas they are striving to improve:

- Agile risk and compliance
- Dynamic risk assessment
- Consumer Finance Protection Bureau (CFPB) exam readiness
- Stress testing for Comprehensive Capital Analysis and Review (CCAR) and/or the Dodd-Frank Act Stress Test 2017 (DFAST)
- Model risk management
- Anti-Money Laundering (AML) and Bank Secrecy Act (BSA).

[1] The full cross-industry report of the findings from Protiviti's Internal Audit Capabilities and Needs Survey, *Embracing Analytics in Auditing*, can be found here: www.protiviti.com/UK-en/insights/internal-audit-capabilities-and-needs-survey.

While these issues figured prominently among the very top concerns in our findings, respondents also identified numerous other internal audit areas — some unique to the FSI (e.g., derivatives and hedging), others unique to financing activities (e.g., the current expected credit loss [CECL] accounting standard) and still others applicable across all industries (e.g., the updated cloud computing accounting standard) — they intend to strengthen in the coming months. We have organized the chapters and call-outs that follow to reflect the priorities and focal points respondents identified.

1. **Cybersecurity:** Robust Cybersecurity Programs Required
2. **Technology:** Supporting Innovation Through Risk-Based Technology Auditing
   - Auditing the Cloud Requires Strategic Clarity
   - Mobile and Digital's Speed and Convenience Risks
3. **Stress Testing:** Regulators Stress Internal Audit's Role in Model Risk Management
   - Data Analytics Capabilities Go Deeper
4. **Model Risk Management:** Addressing CECL Requirements
5. **Risk Management:** Evolving Opinions: An Agile Approach to Assessing Enterprise Risk
6. **Facing the Future with Confidence:** Responding to Regulatory Volatility and Other Emerging Risks
   - Emerging Risks Get Political
   - BSA/AML Gets Programmatic (and Personal)
   - CFPB Examination Readiness Requires Regulatory Agility
7. **In Closing**

Recent political swings, the uncertainty of regulatory change and the never-ending disruptions sparked by technology's onward march have combined to make the future of the FSI more daunting, more promising and more uncertain than ever. The near-term future of U.S.-based financial regulation represents just one of many factors that CAEs and their functions are focusing on. While internal auditors cannot project the future state of financial regulation, their work can help ensure that the organization remains equipped to handle likely regulatory shifts.

To do so, the function needs to have the leadership, strategy, processes, technology and relationships in place that enable it to continually monitor how *all* emerging risks, including regulatory changes, along with all other elements of the organization's risk taxonomy, are developing. The findings and analyses that follow in this report are designed to help FSI internal auditors ensure that their organizations are prepared for an unknowable future.

Robust Cybersecurity Programs Required

Matthew Mueller
Managing Director,
Internal Audit and
Financial Advisory.

Adam Hamm
Managing Director, and former president of the National Association of Insurance Commissioners (NAIC) and former chairman of its Cybersecurity Task Force.

Andrew Retrum
Managing Director,
Technology Consulting.

Internal audit also plays a key role in figuring out what cybersecurity regulations require, the extent to which the company currently meets those requirements and what, if any, gaps need to be addressed. Fulfilling this role requires a significant amount of expertise and knowledge.

— Matthew Mueller, Protiviti Managing Director

The chief information security officers (CISOs) who participated in a recent Protiviti panel discussion responded swiftly when their audience of internal auditors asked how they could help fortify organizational cybersecurity: "Don't wait for us to call you," one of the CISOs responded. "Help us identify what the most pressing cybersecurity issues are, and then help us fix them."

Internal auditors are hungry for these types of insights — and collaborations — as they strive to improve their technical knowledge concerning one of the most troubling risks confronting all organizations today. In this year's survey, respondents identified the AICPA's Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program as the top general technical knowledge area they are targeting for improvement; cybersecurity risk/threat knowledge also was identified as a top-five improvement priority. Another half-dozen or so of the survey's top technical-knowledge improvement priorities also focused on, or directly affected, cybersecurity, including *Auditing Smart Devices and Assessing Cybersecurity Risk,* two of The IIA's Global Technology Audit Guides (GTAGs); digital transformation; mobile applications; the Internet of Things; the NIST Cybersecurity Framework; and ISO 2700 (information security).

As internal auditors work to strengthen their cybersecurity-related assessments, two issues loom large: the quickly changing regulatory landscape and internal audit's need to collaborate with information security colleagues and other parts of the organization. "The regulatory aspect is crucial," says Protiviti managing director Adam Hamm, who points to rules recently finalized by the New York Department of Financial

Services (NYDFS) earlier this year. Under these rules, banks, insurers and other financial services regulated by the NYDFS must maintain a robust cybersecurity program with well-defined risk assessments to protect consumers and ensure the safety and soundness of New York State's FSI.[2]

"New York is the first state to adopt comprehensive cybersecurity regulation," says Hamm, who expects other states to follow suit. Hamm also notes that the National Association of Insurance Commissioners (NAIC) is finalizing its highly anticipated cybersecurity model law.

• • • *General Technical Knowledge (top 10 areas)*

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level (5-pt. scale)
1 (tie)	**AICPA'S Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (Exposure Draft)**	1.9
	Cloud Computing	2.4
3 (tie)	Cloud Computing Accounting Standard — (Accounting Update 2015-05—Intangibles—Goodwill and Other—Internal-Use Software (Subtopic 350-40): Customer's Accounting for Fees Paid in a Cloud Computing Arrangement)	1.8
	Big Data/Business Intelligence	2.4
	Cybersecurity Risk/Threat	2.8
6	**GTAG: *Auditing Smart Devices: An Internal Auditor's Guide to Understanding and Auditing Smart Devices***	2.0
7 (tie)	Business/Digital Transformation	2.3
	Mobile Applications	2.5
9 (tie)	Auditing Corporate Culture	2.6
	Internet of Things	2.4

[2] "New York Steps Up With First State-Level Cybersecurity Regulations for Financial Services Companies," March 8, 2017: https://blog.protiviti.com/2017/03/08/new-york-steps-up-with-first-state-level-cybersecurity-regulations-for-financial-services-companies/.

The NYDFS cybersecurity rules call for companies to designate a qualified chief information security officer (CISO) to administer the cybersecurity program. While larger financial institutions typically have CISOs and information security functions, smaller entities may need to make structural changes in order to comply. For their part, internal audit functions are finding value in deepening their relationship with CISOs and other key cybersecurity stakeholders on the board, in the business and within the company's vendor ecosystem. "Internal auditors should proactively work with the CISO on cybersecurity," says Protiviti managing director Andrew Retrum. "That means working hand-in-hand with the CISO before and after formal audits take place."

CISOs understandably struggle to manage all of the security risks flaring up amid the widespread adoption of new technology in their organizations. And security officers frequently require assistance in keeping pace with new cybersecurity regulations. "Internal audit also plays a key role in figuring out what cybersecurity regulations require, the extent to which the company currently meets those requirements and what, if any, gaps need to be addressed," says Protiviti managing director Matthew Mueller. "Fulfilling this role requires a significant amount of expertise and knowledge."

Internal audit's collaborations at the board level can also help strengthen cybersecurity. Recent cross-industry Protiviti research indicates that organizations with board members who engage in IT security matters and organizations with all core security policies in place rate significantly higher than other companies in nearly all facets of information security capabilities. While internal audit leaders can help foster board engagement and ensure that cybersecurity policies are effective, they should keep in mind that these policies should be supported with effective training programs and communications throughout the organization, given the frequency with which human fallibility enables cyber breaches. The same research also highlighted two pervasive cybersecurity shortcomings that hamper organizational cybersecurity: subpar data classification and management programs, and ineffective vendor risk management capabilities. FSI internal audit functions should focus on both of these areas in their IT security work.[3]

Despite the fact that this work involves complex technology and a rapidly growing number of regulatory-compliance requirements, internal audit should maintain its unique perspective on people, processes and high-level governance when striving to strengthen cybersecurity. "Cybersecurity compliance requirements are increasing," Mueller adds. "But this is not just about complying with the rules or working through a list. This is about making sure the organization has the right security governance, processes, controls and mindset in place."

[3] *Managing the Crown Jewels and Other Critical Data: Protiviti's 2017 Security and Privacy Survey*: www.protiviti.com/sites/default/files/united_states/insights/2017-it-security-privacy-survey-protiviti_0.pdf or this link: https://www.protiviti.com/US-en/insights/it-security-survey.

Impacts on Internal Audit

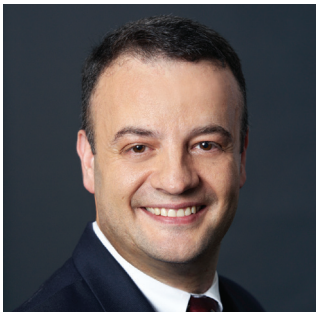
Cyber threats are intensifying. In response, regulators at every level are putting forth new regulations that lay out more specific practices and processes for financial services organizations and their internal auditors to follow. While regulatory compliance is becoming a crucial aspect of cybersecurity, internal auditors should help their organizations embrace much more than a check-the-box approach to cybersecurity.

Action Items for Chief Audit Executives and Internal Audit Functions to Consider When Assessing — and Addressing — Cybersecurity

1. Work with management and the board to develop a cybersecurity strategy that reflects and addresses current information and privacy policy.
2. Recognize that organizations whose boards actively engage in IT security issues tend to operate more effective cybersecurity capabilities compared to organizations whose boards are not engaged in IT security.
3. Ensure that cybersecurity risk is fully integrated into the audit universe and audit plan based on the current risk it represents to the organization.
4. Proactively collaborate with the CIO and CISO on cybersecurity matters to help identify and manage potential risks before threats materialize.
5. Monitor new cybersecurity regulations from state and federal authorities wherever the organization operates and ensure that the internal audit function is kept informed of all relevant rules and rule updates.
6. Identify and address skills and expertise gaps related to cybersecurity within the internal audit function.
7. Ensure that data classification and management capabilities as well as vendor risk management approaches are sufficiently robust to enable the organization to address cyber risks as effectively and efficiently as possible.
8. Develop a strategy with audit to review the various components of cybersecurity and support a conclusion on its effectiveness.
9. Review second-line programs and frameworks to help ensure policy is aligned to organizational risk appetite.
10. Determine appropriate structure to review cyber-security from the top down while also supporting internal audit teams in assessing implementation on security within individual audits.

Supporting Innovation Through Risk-Based Technology Auditing

Tyrone Canaday
Managing Director,
Technology Consulting.



James Armetta
Managing Director,
Internal Audit and
Financial Advisory.

Internal audit should take a risk-based approach to prioritizing their audits of emerging technology areas while applying as much continuous monitoring to high-priority technology risks as possible.

— Tyrone Canaday, Managing Director

Technology is evolving more rapidly than most of us can comprehend. Within a decade, so-called augmented-humanity products — offerings that integrate digital technology with biological systems — will hit the consumer market, according to IDC.[4] Less astounding forms of new technologies such as cloud, mobile, data analytics and social media already are transforming the industry. Within three years, IDC projects, 67 percent of all enterprise information technology (IT) spending will target cloud-based products and services (see "Auditing the Cloud Requires Strategic Clarity" below). Within two years, 40 percent of digital transformation efforts and 100 percent of Internet of Things (IoT) initiatives will be supported by some form of artificial intelligence. By 2018, 75 percent of IT development teams will integrate AI functionality into one or more software applications. Today, nearly one-third of marketing functions within large consumer companies are tinkering with augmented reality (AR) and virtual reality (VR).

Financial services organizations need to remain on the leading edge of these technology-adoption trends. Consumers are shifting from physical locations to digital channels. Financial technology (fintech) companies pose new competitive threats as well as partnership and investment opportunities. More traditional financial organizations are adapting their research and development (R&D) processes and technology-development capabilities to churn out advanced products and services to fulfill rapidly changing customer expectations.

This qualifies as good and bad news. The massive customer-experience and profitability benefits that cloud, big data, IoT, AI, AR, VR, robotics and other emerging technologies can deliver are accompanied by new risks. This explains why survey respondents identified audit process knowledge regarding auditing new technologies as a top-three improvement priority.

[4] *IDC Sees the Dawn of the DX Economy and the Rise of the Digital-Native Enterprise*, Nov. 1, 2016: www.idc.com/getdoc.jsp?containerId=prUS41888916.

- - - *General Technical Knowledge (top 10 areas)*

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level (5-pt. scale)
1 (tie)	AICPA'S Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (Exposure Draft)	1.9
	Cloud Computing	2.4
3 (tie)	Cloud Computing Accounting Standard — (Accounting Update 2015-05—Intangibles—Goodwill and Other—Internal-Use Software (Subtopic 350-40): Customer's Accounting for Fees Paid in a Cloud Computing Arrangement)	1.8
	Big Data/Business Intelligence	2.4
	Cybersecurity Risk/Threat	2.8
6	GTAG: *Auditing Smart Devices: An Internal Auditor's Guide to Understanding and Auditing Smart Devices*	2.0
7 (tie)	**Business/Digital Transformation**	2.3
	Mobile Applications	2.5
9 (tie)	Auditing Corporate Culture	2.6
	Internet of Things	2.4

• • • *Audit Process Knowledge (top 10 areas)*

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level (5-pt. scale)
1	Data Analytics Tools: Data Manipulation	2.8
2	Data Analytics	3.0
3	**Auditing IT: New Technologies**	2.7
4	Fraud: Fraud Risk Assessment	2.9
5 (tie)	Data Analytics Tools: Statistical Analysis	2.8
	Fraud: Fraud Detection/Investigation	2.9
	Continuous Monitoring	3.0
8	Auditing IT: Security	3.0
9 (tie)	Continuous Auditing	3.0
	Fraud: Monitoring	2.9

Auditing the Cloud Requires Strategic Clarity

Cloud computing marks a major focal point for internal auditors, for good reason. Survey respondents identified cloud computing and the Financial Accounting Standards Board's (FASB's) cloud computing accounting standard as top technical knowledge areas they targeted for improvement this year.

Both priorities make sense given the rapid, widespread adoption of cloud-based software, infrastructure and platforms by most businesses, especially those within the FSI, where information technology functions contend with significant "Do much more with less" pressure. To optimize the agility, innovation and cost-efficient returns on their organization's growing investments in cloud technology, IT functions, risk managers and internal auditors must address a wide range of risks, including those related to cybersecurity and data privacy, regulatory compliance, and vendor risk management, among others.

"Vendor risk management is a huge component of assessing, managing and monitoring risks related to cloud technology," says Protiviti Managing Director Tyrone Canaday. Keeping current on new and emerging regulatory compliance requirements marks a major component of a robust third-party risk management (3PRM) program. Investing in third-party cloud product and services offerings can help organizations shift capital expenditures on large data center buildouts to operational expenditures that can align more efficiently with business demand. Yet, this shift must be conducted in adherence to relevant accounting rules.

Those rules, as well as related regulations and standards, can be difficult to comply with amid busy enterprisewide digital transformation efforts that often involve the frequent onboarding of new vendors, bimodal IT environments, systems integration initiatives, core modernization efforts and other complications. "Organizations should start with a strategy for cloud adoption that aligns with business strategy and business objectives," Canaday adds. "Internal audit's activities also should start with that document."

Despite the hyper-advanced nature of these new technologies, managing their downside threats requires engaging the same fundamentals that risk managers and internal auditors routinely apply to old-fashioned risk areas. "Many of these new technologies produce data that organizations use in their applications," says Protiviti managing director Tyrone Canaday. "That means that organizations need to monitor inputs and outputs of the software as well as any unexpected behaviors related to those inputs and outputs."

Canaday emphasizes that some forms of new technology, such as AI and machine learning, require continuous monitoring because of their ability to generate new insights, applications and processes. The intensity of monitoring and attention that internal audit applies to new technologies should correlate with the magnitude of risks they pose to the organization. "Internal audit should apply the same risk-based approach it uses to assess non-technology risks," says James Armetta, a managing director with Protiviti's Internal Audit and Financial Advisory practice. "If machine learning supports a process that does not involve customer data or have a direct impact on revenue, it may qualify as a lower auditing priority. If machine learning affects key data assets — the organization's crown jewels — internal audit needs to closely monitor the controls around that application."

This monitoring requirement extends to the external partners financial services organizations are partnering with more frequently to leverage cloud offerings, data and a range of emerging technology capabilities.

While these third-party relationships can significantly enhance a financial institution's innovation capacity, organizations should practice "responsible innovation," a term the U.S. Office of the Comptroller of the Currency (OCC) defines in guidance regarding fintech companies.[5] This responsibility can be fulfilled according to guidance on third-party risk management practices released in the past year by the OCC, the Federal Reserve, the Federal Financial Institutions Examination Council (FFIEC) and the CFPB.[6]

A robust program addresses risk throughout the 3PRM lifecycle, beginning with the R&D/planning process through due diligence, contracting and onboarding, and monitoring through termination. Specific risk assessment management practices within each of those 3PRM lifecycle phases help financial organizations navigate relevant regulations and manage relevant risks while maintaining the speed and flexibility these partnerships need to produce responsible innovation.[7]

Generating responsible innovation from emerging technologies used inside the financial institution requires similar rigor from an internal audit perspective. "Auditing these new technologies requires an understanding of the nature of these advancements and their impacts to the organization as well as a current understanding of the regulatory requirements that apply to these technologies," Canaday adds. "Internal audit should take a risk-based approach to prioritizing their audits of emerging technology areas while applying as much continuous monitoring to high-priority technology risks as possible."

Impacts on Internal Audit

Internal audit needs to be on the forefront of understanding new technologies and the risks they pose to the organization. They should be regularly monitored and included in the audit plan when deemed necessary based on a risk assessment.

Action Items for Chief Audit Executives and Internal Audit Functions to Consider

1. Establish routines with those responsible for innovation (e.g., chief information officer, chief technology officer or chief innovation officer) to understand the pipeline of emerging technologies being considered or already adopted.
2. Attend senior management committee meetings where emerging technologies are discussed to form a view of all risks and to ensure they are being managed prior to adoption and are aligned with the organization's strategy.
3. Increase the use of continuous monitoring of technologies whose inputs, outputs and surrounding behaviors represent significant risks.
4. For third parties engaged to develop, host or manage emerging technologies, ensure vendor management is effectively assessing risk, appropriately classifying the third party, and applying risk management practices and procedures based on their classification.

[5] *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, U.S. Office of the Comptroller of the Currency, March 2016: www.occ.gov/publications/publications-by-type/other-publications-reports/pub-responsible-innovation-banking-system-occ-perspective.pdf; *Recommendations and Decisions for Implementing a Responsible Innovation Framework*, OCC, Oct. 2016: www.occ.gov/topics/bank-operations/innovation/recommendations-decisions-for-implementing-a-responsible-innovation-framework.pdf; and *Exploring Special Purpose National Bank Charters for Fintech Companies*, OCC, Dec. 2, 2016: www.occ.gov/topics/bank-operations/innovation/special-purpose-national-bank-charters-for-fintech.pdf.

[6] Ibid.

[7] See *Enabling Speed of Innovation Through Effective Third-Party Risk Management*: www.protiviti.com/3prm.

5. Monitor developments in regulatory guidance for emerging technologies in the portfolio and consider this guidance in future audit activity.
6. Recognize that cloud, artificial intelligence, machine learning, data analytics, IoT, robotics and other forms of emerging technologies frequently give rise to multiple risks, including issues related to data integrity, data privacy, cybersecurity, regulatory compliance, vendors and more.
7. When focusing on technology partners, manage risks across the entire 3PRM lifecycle.
8. Monitor new and emerging regulatory guidance and requirements regarding third-party risks and relationships.

Mobile and Digital's Speed and Convenience Risks

Customers of all kinds are absolutely delighted by speed and convenience. In the consumer banking sector, for example, online and mobile self-service offerings are greatly enhancing customer experience, particularly among both younger and higher-income customer segments.[8]

To sustain these valuable digital experiences, banks must keep pace with rapidly changing technologies, and this requires financial services organizations to transform how they develop new apps and software, which external vendors they partner with, where they source data and how they protect it. While this transformation is centered within the IT function, its ripple effects — and risks — extend to risk managers, compliance professionals and internal auditors. These challenges cover IT risks, operational risks, vendor risks, compliance risks, reputational risks and even strategic risks.

So, it is unsurprising that internal auditors in the FSI have identified business/digital transformation and mobile applications as areas in which they want to strengthen their technical knowledge, according to Protiviti's 2017 Internal Audit Capabilities and Needs Survey.

"The industry's digital transformation is all-encompassing," says Canaday. "There are continually more sensors out there collecting data that financial services organizations use. Mobile devices are also collecting more consumer information. If you're leveraging the Internet of Things and using new types of customer data, you likely have to redo your risk calculations. Institutions need to know if the data and information they're using to making key decisions regarding trading, customers and products are credible."

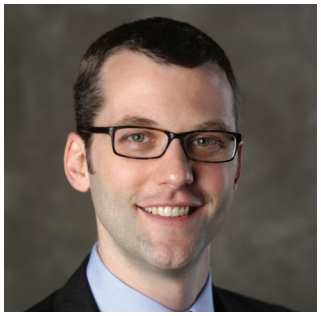
Internal audit's recalculation of IT risks in the new era of mobile-device ubiquity and data analytics also should extend to the new approaches IT functions are using to develop new products and capabilities. As the adoption of agile software development methodologies increases, IT auditor functions will need more Agile expertise and a firm understanding of the qualities that can make (top-notch project management skills) or break (skills deficiencies and organizational silos) Agile implementations.

FSI organizations and their IT functions are moving quickly to respond to heightened customer demands for greater speed and convenience. Internal audit functions need to keep pace while keeping tabs on new risk and vulnerabilities that accompany that response.

[8] *Getting to the Heart of Customer Experience: Insights from Protiviti's Annual Consumer Banking Survey*, Protiviti, 2016: www.protiviti.com/es/node/73906.

Regulators Stress Internal Audit's Role in Model Risk Management

Barbi Goldstein
Managing Director,
Internal Audit and
Financial Advisory.



Todd Pleune
Ph.D., Managing Director,
Data Management and
Advanced Analytics.

Regulatory pressure on audit to do more around stress testing has been mounting in the past 12 months . . . [T]here is an idea among regulators that internal audit can do more to ensure that the organization's stress testing is even more robust.

— Todd Pleune, Protiviti Managing Director

Stress testing has FSI internal auditors feeling more regulatory pressure these days. Internal auditors participating in Protiviti's 2017 Internal Audit Capabilities and Needs Survey pinpointed stress testing as the number one area in which they want to improve their audit process knowledge. This sentiment reflects regulators' heightened expectations regarding the internal audit function's assessments of stress testing and capital planning.

"Regulatory pressure on audit to do more around stress testing has been mounting," reports Protiviti managing director Todd Pleune. "Internal audit's primary responsibility is to test the controls surrounding stress-testing processes, and I think that testing has been fairly strong. Now, there is an idea among regulators that internal audit can do more to ensure that the organization's stress testing is even more robust." Improving internal audit's assessments of stress tests starts with the function ensuring that the organization has an effective model risk management (MRM) policy in place.

Changes in MRM policies and model governance infrastructures are being driven by a number of regulatory bodies around the world, including Basel III and the European Market Infrastructure Regulation (EMIR). In the U.S., financial institutions are busily responding to guidance on model risk, model governance and stress testing issued by the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC) and the OCC. The risk capital that institutions must hold is subjected to periodic stress testing via Comprehensive Capital Analysis and Review (CCAR) and the Dodd-Frank Act Stress Test (DFAST) results. (The Federal Reserve evaluates the stress testing and capital planning processes of U.S. banking organizations with assets greater than $10 billion through DFAST and organizations with assets of $50 billion or more through CCAR; many institutions must comply with both CCAR and DFAST.)

• • • *Audit Process Knowledge – U.S. Financial Services Industry (top 10 areas)*

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level (5-pt. scale)
1	Stress Testing (CCAR/DFAST)	2.2
2	Current Expected Credit Loss (CECL)	2.0
3	Derivatives and Hedging	2.2
4	Derivatives and Securities	2.3
5 (tie)	Capital Planning	2.3
	Mergers and Acquisitions Due Diligence	2.3
7	Securitizations	2.2
8 (tie)	Capital Markets Planning	2.3
	International Regulation	1.9
10	Asset Liability Management /Liquidity Management	2.4

These stress tests require financial institutions to produce forward-looking projections for credit losses, balance sheet/income statement and other variables based on forward-looking scenarios for various macroeconomic variables. The projections must be mathematically appropriate and useful for business decision making. Models must be well-designed, validated, controlled and fit for the specific purpose of stress testing.

Regulators have made it clear that data completeness and data quality are crucial, and banks continue to invest significant resources and effort improving their data-governance and data-management capabilities to produce DFAST and CCAR reports. As is the case with other risk models, the CCAR and DFAST models must be developed, implemented, governed and validated per SR 11-7 and OCC 2011-12 "Supervisory Guidance on Model Risk Management."

Data Analytics Capabilities Go Deeper

Despite the intense focus on data analytics FSI internal auditors have demonstrated in recent years, they remain more committed than ever to improving their knowledge of data analytics and related tools.

This year's survey respondents identified data analytics as the top technical knowledge area as well as the top audit process knowledge area they are targeting for improvement. Data analytics tools (for data manipulation and statistical analysis), continuous monitoring and continuous auditing also ranked as top audit process knowledge areas that respondents want to improve. Amid the recent volatility of the political, regulatory and economic realms that influence the FSI, internal audit's investments in data analytics knowledge, tools and processes remain remarkably consistent.

"Regardless of the changes that actually result from the current volatility and uncertainty, financial services organizations will continue to enhance the way they use analytics," says Barbi Goldstein, a managing director with Protiviti's Internal Audit and Financial Advisory practice. "The need to better understand the organization's changing risks will never go away, regardless of how the regulatory environment changes. To succeed, companies need to manage all of their strategic risks, reputational risks and every other form of risk. Data analytics approaches and tools as well as continuous auditing and monitoring capabilities help businesses successfully manage all risks."

Goldstein's point is supported by the cross-industry findings from Protiviti's 2017 Internal Audit Capabilities and Needs Survey. These findings show that internal audit functions with more advanced continuous auditing and monitoring capabilities tend to produce stronger risk assessments, more effectively track fraud indicators and key operational risk indicators, and maintain more of a real-time view of organizational risk compared to organizations with less sophisticated analytics, auditing and monitoring capabilities.

Although financial services internal audit functions tend to boast more developed analytical capabilities than internal audit shops in other industries, elevating these programs to a higher level of sophistication remains a challenge. One reason for that, Goldstein points out, relates to the fierce competition for expertise and talent. "Not so long ago, analytic talent referred to an IT auditor who had learned how to use continuous auditing software," Goldstein says. "Today, financial services industry internal audit functions are competing for data scientists."

Creating a formal analytics strategy, developing a roadmap and operating a dedicated analytics function mark effective ways to advance internal audit's analytics capabilities. This progress is crucial given the strides that competitors are notching. "The most advanced functions in the industry are increasing their use of predictive analytics to help them identify unfolding risk areas that require more of their time and attention," Goldstein adds.

To fulfill regulators' requirements — and their heightened expectations — concerning CCAR and DFAST, internal audit functions within financial services organizations must work through several common model risk management challenges, including accessing the quantitative expertise necessary to determine if model validations were conducted appropriately, maintaining data quality and availability, and ensuring that independence is maintained between teams that develop the models and those who validate the models.

These challenges can be present within institutions of all sizes. That said, the largest institutions tend to have relatively mature model risk management governance infrastructure in place; their main challenge relates to expertise and speed — access to specialized expertise that can help complete model development and validation in a timely fashion.

Many mid-sized organizations must address the more comprehensive challenge of building out their model risk infrastructure, which may involve forming a model risk oversight committee comprised of risk managers, modelers and business owners. Internal audit frequently serves in a nonvoting capacity on these committees. The risk model skills gaps within mid-sized as well as smaller banks can be severe. The smaller organizations compete for skills as well as for external experts who specialize in mode development, model testing and/or internal audit support — and who have more than enough work at the moment.

Impacts on Internal Audit

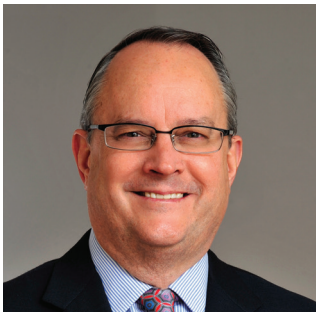
Internal audit has a key role to play in ensuring that the organization has an effective model risk management (MRM) policy in place, one that supports DFAST and CCAR requirements.

Action Items for Chief Audit Executives and Internal Audit Functions to Evaluate MRM in Their Annual Audit Plans

1. Ensure that MRM is evaluated within the audit universe and conduct regular model governance audits.
2. Review the overall MRM process governance, design, resources, and adequacy to manage risk within the appetite and tolerances set by the board of directors.
3. Evaluate the extent to which the internal audit function possesses the expertise and resources necessary to challenge the effectiveness of models and review validations for adequacy.
4. Conduct audits of processes that support CCAR and/or DFAST reports with a focus on the data integrity of inputs to their processes.
5. Assess data integrity controls and testing, and evaluate the quality and completeness of source data.
6. Examine that all material risks are covered in stress testing and CCAR, and confirm that all risks are modeled appropriately.

Addressing CECL Requirements

Charles Soranno
Managing Director,
Internal Audit and
Financial Advisory.



Charlie Anderson
Managing Director, Model
Risk and Capital Management,
Data Management and
Advance Analytics.

Benjamin Shiu
Associate Director,
Data Management and
Advance Analytics.

This is a scarce skill set. It requires high-level quantitative knowledge and advanced techniques. It's difficult for any part of the business, including internal audit, to find people with those skills right now.

— Charlie Anderson, Protiviti Managing Director

Although fresh regulatory guidance concerning the Financial Accounting Standards Board's (FASB's) new current expected credit loss (CECL) methodology for estimating credit losses under U.S. generally accepted accounting principles (U.S. GAAP) has appeared in the past 12 months, internal audit's CECL-related priorities remain unchanged. As was the case in last year's survey, 2017 FSI internal auditors identified CECL as a top area they are targeting to improve their audit process knowledge.

This expertise is in short supply, due to its highly technical nature. CECL know-how is also in high demand given that the new credit impairment accounting standard will be applied to a broad range of organizations — financial services companies as well as companies that issue loans and financing in other industries.

"This is a scarce skill set," notes Protiviti managing director Charlie Anderson. "It requires high-level quantitative knowledge and advanced techniques. It's difficult for any part of the business, including internal audit, to find people with those skills right now."

Many financial services organizations are grappling with that expertise challenge as they struggle to build new risk models necessary to generate the more forward-looking "expected loss" approach for recognizing credit losses that the CECL methodology entails. The new standard takes effect for public business entities (PBEs) beginning in January 2020 and for non-PBEs a year later.[9] The new risk models the standard requires are more sophisticated and they require more data compared to the "incurred loss" approach that CECL replaces. "Some organizations are encountering difficulties in the data-collection stage.

[9] Charles Serrano, "Four U.S. Regulatory Agencies Issue CECL FAQs — Here Is the Summary," the Protiviti View, https://blog.protiviti.com/tag/cecl-methodology/.

"This is especially the case for smaller to mid-sized organizations," notes Protiviti Associate Director Benjamin Shiu. In addition to collecting historical data, organizations need to update their data-sourcing and data-governance processes to support these new data-collection requirements.[10]

Organizations also should evaluate whether they need to redesign other processes and systems. Some companies have discovered that they need to revamp loss-reserve processes to reflect changes in assets classifications, for example.

The updating of analytical methodologies so that they can generate forward-looking and lifetime loan loss forecasts remains one of CECL's most complex challenges. This complexity has recently caused some organizations to question whether risk models for Basel II or CCAR can be leveraged for new CECL models. The answer is that this approach is unlikely to work well; any organization considering this route should proceed with extreme caution. This is the case because CECL, an accounting standard, requires fundamentally different (and generally more conservative) projections.

• • • *Audit Process Knowledge – U.S. Financial Services Industry (top 10 areas)*

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level (5-pt. scale)
1	Stress Testing (CCAR/DFAST)	2.2
2	**Current Expected Credit Loss (CECL)**	2.0
3	Derivatives and Hedging	2.2
4	Derivatives and Securities	2.3
5 (tie)	Capital Planning	2.3
	Mergers and Acquisitions Due Diligence	2.3
7	Securitizations	2.2
8 (tie)	Capital Markets Planning	2.3
	International Regulation	1.9
10	ALM/Liquidity Management	2.4

[10] *Impact of the New Current Expected Credit Loss (CECL) Methodology*, Protiviti, 2016: www.protiviti.com/US-en/insights/pov-cecl-methodology.

As their business and operational colleagues wrestle with tracking down data, revamping analyses and taking other, highly complex steps necessary to update their modeling methodology, internal audit also must advance along the CECL learning curve.

"CECL completely changes the way banks prepare their loss reserves," Shiu says. "Internal audit needs to truly understand what this new accounting standard is, how it affects the business and what CECL models should look like." Many of the quantification elements within the new standard will pose stiff tests to internal audit functions. "Internal auditors will need to go beyond simply auditing the process by which the CECL numbers are produced," Anderson adds. "The models themselves need to be audited, and that work has numerous mathematical and statistical aspects that will challenge internal audit functions."

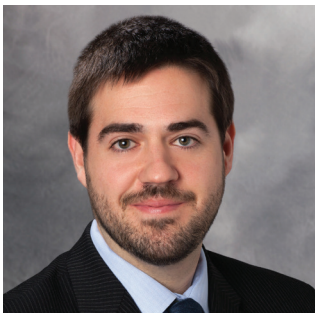
Impacts on Internal Audit

Internal audit functions are in the process of augmenting their CECL-related knowledge as quickly and effectively as possible.

Action Items for Chief Audit Executives and Internal Audit Functions to Consider When Addressing CECL Requirements

1. Ensure that internal audit understands the CECL methodology for estimating credit losses under U.S. GAAP. Consider assigning a champion.
2. Assign someone involved in the CELC initiative to be point person [champion] for understanding the initiative and to act as liaison to other areas, providing the internal audit perspective.
3. Consider auditing the implementation of CECL.
4. Recognize that implementing the CECL methodology requires specialized expertise (with credit risk models, process design, data acquisition, model validation and more) that many organizations will have difficulty bringing onboard in a full-time staff capacity.
5. Identify the key areas for improvement that are necessary to meet CECL requirements.
6. Assess the extent to which the internal audit function will be able to assess new risk models and the extent to which they conform to the CECL methodology.
7. Identify how risk managers have altered data infrastructures and data-collection processes to satisfy CECL requirements.

Evolving Opinions: An Agile Approach to Assessing Enterprise Risk



Matthew Perconte
Managing Director,
Risk and Compliance.

Michael Thor
Managing Director,
Internal Audit and
Financial Advisory.

More organizations are striving to achieve synergies across their three lines of defense, which is a primary objective of what we refer to as Agile Risk Management.

— Matthew Perconte, Protiviti Managing Director

When it comes to assessing, and opining on, the organization's enterprise risk management (ERM) framework and its overall risk management capability, internal audit finds itself in the early rounds of an evolving challenge, the extensive scope of which is becoming more well-defined with each regulatory update.

The key to addressing this challenge is an efficient form of risk management alignment that extends across an organization's first, second and third lines of defense. "More organizations are striving to achieve synergies across their three lines of defense, which is a primary objective of what we refer to as Agile Risk Management," notes Protiviti Director Matthew Perconte. "Internal audit, in its third-line role, is trying to take advantage of other risk management structures, applications and data used by the first and second lines while maintaining independence and providing objective assurance to the board and executive management."

Since the financial crisis, regulators and standard-setters have continually pressed financial services organizations to enhance their systems of risk management. These regulatory authorities also have called on internal audit functions within these firms to provide assurance that risk management systems are in place and operating effectively. In 2014, the OCC, in its heightened standards guidance, clarified that internal audit's role is to opine on the readiness and design of risk management systems' corporate governance structures, including risk culture and risk appetite. OCC Bulletin 2016-47, which revised the *Comptroller's Handbook Booklet*, serves as a more recent example of the growing clarity around internal audit's role in risk assessment.[11] This guidance from the OCC,

[11] *OCC Bulletin 2016-47 — Revised Comptroller's Internal and External Audits Handbook Booklet and Rescissions* Protiviti, Jan. 24, 2017: www.protiviti.com/US-en/insights/occ-bulletin-2016-47-revised-comptrollers-internal-and-external-audits-handbook.

which is based on its previously published heightened standards for some large institutions as well as the Basel Committee on Banking Supervision's (BCBS') internal audit guidance, helps explain why ERM frameworks, along with several other risk areas (e.g., dynamic risk assessment), represent a top improvement priority among survey respondents.

As regulators provide more feedback on internal audit's increasingly comprehensive risk assessments, internal audit leaders are gaining a better understanding of the challenges they need to address to issue accurate opinions on the effectiveness of risk management as well as practices they can deploy to become more responsive in their assessment of a broad collection of risks. Just as more financial services organizations are embracing the Agile Risk Management philosophy to strengthen their system of risk, so, too, are more internal audit functions managing talent and technology in ways that help them align with first and second lines of defense to establish and sustain a forward-looking assessment of risk.

• • • *Audit Process Knowledge – U.S. Financial Services Industry (top 10 areas)*

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level (5-pt. scale)
1	Data Analytics	3.0
2	Dynamic Risk Assessment	2.7
3 (tie)	Anti-Money Laundering and Bank Secrecy Act	2.0
	Enterprise Risk Management Frameworks	2.6
5	Basel Guidance on Internal Audit	2.5
6	CFPB Examination Readiness	2.3
7	Fraud Risk Management	2.8
8	Fair Lending	2.3
9 (tie)	Regulatory Guidance on Internal Audit	3.0
	Interest Rate/Market Risk	3.1

"We have seen a number of internal audit functions integrated into activities earlier in certain key processes in order to provide a more forward-looking understanding of organizational risk," says Michael Thor, a managing director with Protiviti who leads the firm's North American Internal Audit and Financial Advisory practice. "Some internal audit functions participate in strategic planning, for example, to make sure that risks are identified and addressed throughout that planning process."

Developing a forward-looking view of risk can be difficult given the comprehensive nature of internal audit's opinion on the effectiveness of risk management. This assessment covers ERM frameworks, specific operational risks (several of which often require their own targeted audits), model risk management, interest rate and market risk, fraud risks, risk appetites, risk cultures, and more. Although the recent guidance from the OCC and Basel help internal audit functions understand how to aggregate first- and second-line risk assessments and information to inform their opinions, challenges remain.

Access to the expertise needed to assess technical risk areas, such as model risk management, marks a pervasive challenge. To address this need, more internal audit functions are enlisting third parties to supply various types of technical expertise. Aligning risk management mindsets, methodologies and tools across the three lines of defense — and especially between risk management and internal audit — represents another pervasive challenge. "In some organizations, internal audit's assessment and risk management's assessment produce very different sets of insights — due to the use of different methodologies, different supporting technologies and different control taxonomies," Perconte says. "While internal audit's opinion on the effectiveness of risk management is independent, there should be alignment between internal audit and risk when it comes to how organizational risk is viewed, organized and classified."

In organizations where this alignment exists, the business, risk and internal audit use the same language to define, monitor and manage risks; they also tend to leverage the same technology platforms, tools and data models. Establishing this synergy requires time and effort. Internal audit traditionally focused more on the first-line business units when assessing risk; second-line risk management groups are less experienced working with internal audit. By focusing on improving their collaborations, risk and internal audit are better positioned to conduct their individual risk assessments of the business units more efficiently and less disruptively.

This type of Agile Risk Management mirrors the growing agility with which business units operate. Some leading internal audit functions recruit business and risk professionals from other parts of the organization to enhance the function's knowledge of processes and mindsets within the first and second lines. Leading internal audit practices also tend to develop advanced data analytics and continuous auditing and monitoring capabilities, which equip them with more accurate and timelier data to help evaluate risks. "More internal audit functions are asking how they can develop their analytics functions so that they can gain more foresight into potential risks emerging within the organization," Thor adds. "And they're using those insights to continuously adjust their plans to audit specific areas of risk rather than relying on static plans."

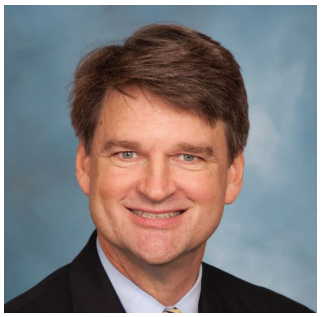
Impacts on Internal Audit

Internal audit's responsibility to opine on the readiness and design of organizational risk management systems and governance structures requires a comprehensive yet efficient risk-assessment work throughout the organization.

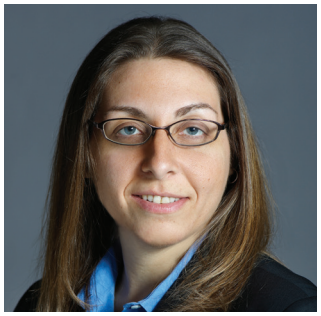
Action Items for Chief Audit Executives and Internal Audit Functions to Consider When Assessing and Opining on Enterprise Risks

1. Support the creation of a unified risk management operating model with clear first-, second- and third- line accountabilities.
2. Fully understand the organization's risk appetite statement and framework — and the extent to which strategic planning (and three- and five-year strategic plans) reflect this risk appetite and capacity.
3. Develop an approach to assess the effectiveness of the risk management framework. Seek to align within the framework developed with the second line of defense.
4. Look for opportunities to integrate internal audit in key business processes and activities that have significant impacts on organizational risk.
5. Actively work toward greater alignment of risk thinking, methodologies, processes, supporting tools and technology systems, and data/indicators across all three lines of defense.
6. Pay particularly close attention to interactions and collaborations between third-line internal auditors and second-line risk managers, many of whom are not accustomed to aligning with each other.
7. Consider elements of the Agile Risk Management philosophy and methodology to strengthen alignment and improve synergies among the three lines of defense.
8. Recognize that regulators expect to see links between risk appetites and capital stress tests that demonstrate an ability to hold the necessary amount of capital in a stressed environment.
9. Identify new indicators and metrics that can help in the measurement, monitoring and management/remediation of risk culture.

Responding to Regulatory Volatility and Other Emerging Risks



Scott Jones
Managing Director,
Internal Audit and
Financial Advisory.



Barbi Goldstein
Managing Director,
Internal Audit and
Financial Advisory.

Internal audit departments should constantly evolve and innovate to maintain an accurate picture of risk — especially emerging risks.

— Barbi Goldstein, Managing Director in Protiviti's Internal Audit and Financial Advisory practice.

Effectively addressing emerging risks requires internal audit functions to operate with a savvy blend of agility, consistency and innovation.

The need to maintain this balance has intensified during a period of political, legislative and economic volatility. A number of high-stake political shifts — including the Brexit vote, recent elections in the U.S. and France, and more — require internal audit to respond to new external risks that may arise from these events. Internal audit also should ensure that the ramifications of these risks, along with emerging risks related to strategic pivots and marketplace shifts, are understood and managed in a consistent manner throughout the organizations. "CAEs are under growing pressure to understand emerging risks, figure out how to integrate them into their auditing work and articulate the potential impacts of these issues to the rest of the organization," says managing director Michael Thor, who leads Protiviti's North American Internal Audit and Financial Advisory practice.

Uncertainty and timing loom prominently among the many challenges of performing that mandate. Emerging risks typically reside outside the realm of an institution's core risk taxonomy. Plus, their new and often fluid nature makes it difficult to evaluate the nature of their impacts and when these impacts could materialize. This is the case for risks that pose both threats and potential opportunities.

President Trump's largely unexpected election win greatly increased the possibility of a scaling back of U.S. business regulations — particularly financial regulations, and especially those financial rules that apply to regional and community banks buckling under hefty compliance burdens. But the nature and timing of this potential shift remains uncertain. "In December, smaller and mid-sized financial institutions were hopeful that the new political climate would bring some sort of regulatory easing,"

notes Scott Jones, a managing director with Protiviti. "While no one expected immediate relief, it made sense for internal audit functions to build some flexibility into their plans for 2017. By the end of the first quarter, however, it became pretty clear that any substantive easing seems unlikely to occur this year."

Additional political, legislative and geopolitical uncertainties that play out in the months ahead likely will generate new regulatory threats and opportunities. FSI internal auditors should recognize, assess and, where necessary, adjust their activities in response.

"Internal audit has proven adept at decomposing organizational risks and assessing those smaller components individually," Thor says. "Yet, many functions need to improve their ability to recognize emerging risks and changes to the organization's risk profile and then invest their attention to those areas based on their potential impact to the institution. Internal audit needs to be agile enough to react to those changes while making sure new risks are reflected in the audit work and the assurance the function delivers."

CAEs appear well-aware of this need; CAE respondents identified agile risk and compliance as a top general technical knowledge area they want to improve.

That agility also requires consistency from internal audit functions, which should create and continually refine a reliable approach to identifying and addressing emerging risks and adjusting as new risks evolve. Audit plans and activities should appropriately reflect the potential impacts of remerging risk, which change over time. The Dodd-Frank Act qualified as an emerging regulatory risk in the wake of the financial crisis. Today, the goal is not to understand Dodd-Frank's impact, but to comply with the many rules that law created as effectively and cost-efficiently as possible.

• • • *Audit Process Knowledge – U.S. Financial Services Industry (top 10 areas)*

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level (5-pt. scale)
1	Data Analytics	3.0
2	Dynamic Risk Assessment	2.7
3 (tie)	Anti-Money Laundering and Bank Secrecy Act	2.0
	Enterprise Risk Management Frameworks	2.6
5	Basel Guidance on Internal Audit	2.5
6	CFPB Examination Readiness	2.3
7	Fraud Risk Management	2.8
8	Fair Lending	2.3
9 (tie)	Regulatory Guidance on Internal Audit	3.0
	Interest Rate/Market Risk	3.1

On that count, innovation can help. "Internal audit departments should constantly evolve and innovate to maintain an accurate picture of risk — especially emerging risks," says Protiviti managing director Barbi Goldstein. This need explains why survey respondents identified dynamic risk assessment as one of the topmost general technical knowledge areas they want to improve in 2017.

Rather than taking a wait-and-see approach in response to the possibility of deregulatory actions, leading financial services internal audit functions are attending conferences, reading between the lines of regulators' comments, and closely monitoring the behavior of examiners and enforcement officials for leading signals. Internal audit functions within smaller to mid-sized institutions are keeping their eye on the largest, most heavily regulated banks, whose internal audit shops have demonstrated that necessity, in the form of extraordinary compliance burdens, is the mother of innovative compliance and risk management practices.

Leading internal audit functions strive to "build a culture of innovation," Thor adds. "They look for new ways to stay ahead of the next examination and to glean early on what those expectations will be."

Michael Thor
Managing Director,
Internal Audit and
Financial Advisory.

Emerging Risks Get Political

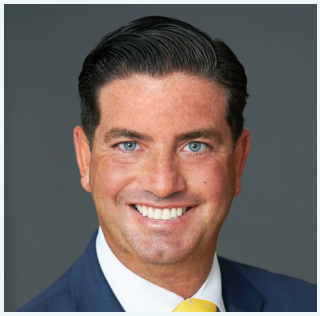
The political changes that have swept through Western countries in the past 18 months feel swift and forceful. The impacts of these shifts on organizational risk, however, are much slower to play out. This gap is of particular concern to internal audit functions, which must integrate the relevant potential impacts of these political shifts into their activities and plans.

The unexpected Brexit vote seemed likely to relocate Europe's financial center from London to Frankfurt, Luxembourg or Dublin. President Trump's election seemed likely to roll back Dodd-Frank while shuttering the CFPB. That neither of these outcomes had materialized months after each event demonstrates the challenge of timing the impacts of political risks and other forms of emerging risks.

"Organizations can't know the precise impact of these types of emerging risks or when these impacts will occur," says Michael Thor, who leads Protiviti's North American Internal Audit and Financial Advisory practice. "Yet, audit committees and other board members are looking for internal audit to help understand these emerging risks and their potential impacts on the organization."

Meeting these board expectations requires an ability to differentiate between signal and noise, a capacity for dynamic risk assessment and a knack for asking the right questions. President Trump's push for tax reform has sparked heated debates on a wide range of contentious issues. From an emerging risk perspective, however, the possibility of a historic corporate tax rate cut would likely increase discretionary spending significantly, and this added cash flow could stimulate M&A activity, which generates new opportunities and risks. Asking how a 15 percent corporate tax rate affects discretionary spending and influences growth strategy is much more effective than taking a wait-and-see approach on whether the reform becomes law.

"Internal audit is in a unique position to look at political changes and understand the change's most important ramifications on the financial services industry and their organization," Thor notes. "When internal audit is tied into risk and strategy at the highest level, it understands how the bank may react to emerging risks that it should be continuously monitoring."



Shaun Creegan
Managing Director,
Risk and Compliance.

BSA/AML Gets Programmatic (and Personal)

For Bank Secrecy Act (BSA)/anti-money laundering (AML) matters, 2016 was a year of intrigue, marked by notable regulatory updates. In May 2016, shortly after the Panama Papers controversy erupted, the Financial Crimes Enforcement Network (FinCEN) issued its final rule on customer due diligence (CDD) and beneficial ownership information.[12] This move adds CDD as the "fifth pillar" to the original four pillars — a system of internal controls, AML compliance officer designation, training, and independent testing — deemed fundamental to an effective AML program. While the timing of the uproar over the alleged hiding of wealth from government regulations and the erection of AML's fifth pillar was a fluke, it drove home the high stakes of BSA/AML compliance.

A couple of months later, those stakes turned personal for chief compliance officers (CCOs) who, according to proposed legislation by the New York Department of Financial Services (NYDFS), would have been subject to criminal penalties when filing incorrect or false annual certifications of transaction monitoring and filtering programs related to BSA/AML.[13] Although the final rule, known as Part 504, removed that CCO-liability provision, it also demonstrated regulators' heightened expectations and aggressive intent concerning AML compliance.

Survey respondents, who ranked BSA/AML as a top technical knowledge area they are targeting for improvement this year, appear well aware of this regulatory intent.

"Regulators increasingly are looking for holistic AML programs rather than situations where organizations assess their AML compliance as a discreet component of an annual audit," says Shaun Creegan, a managing director within Protiviti's Risk and Compliance practice. "I think the days of doing a single AML review and then putting it away for the rest of the year are gone. Regulators want see AML compliance be supported by continuous monitoring that ensures all relevant controls are working effectively. The big word from the regulators right now is 'sustainability.'"

Formal BSA/AML programs typically include governance steering committees, staffing and training plans, documented methodologies, comprehensive coverage requirements, risk and controls matrices, testing schedules, and other key components. "It's also important to use a defined sampling methodology when performing transactional testing," Creegan adds. "Formal programs should cover the entire AML-compliance lifecycle."

[12] "Challenges Posed by FinCen's Final Customer Due Diligence Rule," Protiviti, June 14, 2016: www.protiviti.com/UK-en/insights/fincen-final-rule-collection-beneficial-ownership-information-and-customer-due-diligence.

[13] "NY Dept. of Financial Services' Final Transaction Monitoring and Filtering Program Regulation," Protiviti, July 6, 2016: www.protiviti.com/US-en/insights/new-york-department-financial-services-final-transaction-monitoring-and-filtering-program-0.

Steven Stachowicz
Managing Director,
Regulatory Risk Consulting.

CFPB Examination Readiness Requires Regulatory Agility

In September 2016, the CFPB levied the largest penalties against a financial institution since it started operating in 2011. The punishment targeted illegal sales practices, in particular submitting applications and opening bank accounts for customers without their authorization or knowledge among other practices. This enforcement action highlights the expansive nature of the CFPB's authority to regulate unfair, deceptive or abusive acts or practices (UDAAP), the qualitative nature of which poses challenges to financial institutions to manage, measure and demonstrate compliance with legal and regulatory requirements and ready themselves for regulatory examinations.

"Regulators are increasingly focused on the manner in which financial services industry organizations manage the risks associated with sales practices," notes Steven Stachowicz, a managing director with Protiviti's Regulatory Risk Consulting practice. "Regulators expect organizations to evaluate their compensation and performance management plans and programs to assess what risks these mechanisms may pose to customers. For compliance and internal audit functions, assessments related to sales practices are quite different than traditional, technical compliance reviews that rely on more quantitative measures."

This shift helps explain why survey respondents ranked CFPB examination readiness as a top technical knowledge area requiring improvement.

CFPB examination readiness involves technical compliance with the federal consumer financial laws, such as the Truth in Lending Act and the Fair Credit Reporting Act, among others, as well as how the organization manages its UDAAP-related risks. While the CFPB has published extensive examination procedures that organizations can leverage to measure the effectiveness of their processes and controls, these procedures are highly qualitative for purposes of managing UDAAP and the form and function of compliance management systems generally. Compliance management is not a "one size fits all" proposition, and UDAAP-related risks are not easily inventoried or quantified.

Internal audit continues to have challenges developing and accessing the expertise and resources necessary to address the technical compliance activities required by the CFPB examinations and other regulations. While this is not a new issue, it is compounded by the expanding regulatory focus on qualitative matters as well. "Internal audit departments — and, really, all lines of defense — are being challenged to think beyond technical compliance requirements to evaluate the impact of a wider range of organizational practices on its consumers," Stachowicz notes. "Evaluating an organization's sales practices for technical compliance and UDAAP-related risks is not something that can be accomplished through completing a compliance checklist or reviewing a series of disclosures alone. It involves a broader, more insightful evaluation of corporate governance and specific mechanisms and processes, such as incentive compensation and performance management, and determining how these things influence sales practices and prevent or mitigate compliance risks and harm to customers."

continued...

"UDAAPs are a broad and arguably nebulous concept," Stachowicz notes. "There aren't a lot of bright lines around what qualifies as unfair, deceptive or abusive, and as such there is a lot of hesitancy on the part of compliance officers and internal audit departments to identify something as a UDAAP. When you think about it, though, UDAAP is inextricably linked to corporate culture — if thinking about negative impacts on and consequences to customers of an organization's products, services or practices isn't embedded in its culture, bad things may happen. Internal audit is the last line of defense for an organization, and has to be able to call it like it sees it."

That explains why more organizations are seeking to instill their compliance and audit programs with greater agility so that they can conduct regulatory change management efforts more effectively and efficiently as new rules, guidance, punishments and precedents materialize. It also explains why internal audit functions are striving to stretch their assessments beyond technical compliance matters.

Impacts on Internal Audit

Internal audit functions fulfill a unique and crucial role in enabling the organization to understand emerging risks and how to mitigate their impact.

Action Items for Chief Audit Executives and Internal Audit Functions to Consider When Addressing Emerging Risks and Regulatory Risks

1. Focus on improving dynamic risk assessment capabilities, especially with regard to emerging risks.
2. Assess and continuously improve the agility and efficiency of regulatory compliance efforts.
3. Within larger, global organizations, be aware of the growing tendency for federal regulators in more countries to issue and enforce rules in ways that differ from approaches in other countries.
4. Strive to foster a culture of internal audit innovation with regard to managing regulatory risks and emerging risks.
5. Identify and learn from the most innovative internal audit functions.
6. Closely monitor the behaviors of regulatory examiners as potential indicators of larger changes that may be coming down the pike.
7. Maintain close relationships with risk and compliance colleagues as well as with key external stakeholders and influencers in the regulatory realm.

In Closing

CAEs and internal audit departments will continue to be challenged by new and unexpected risks along with the ongoing need to address core components of their risk taxonomy with greater efficiency and effectiveness. A continuously changing organizational risk environment requires internal audit functions to continuously evolve, innovate and, above all, improve.

When it comes to fulfilling their mission to assess and opine on the readiness and design of organizational risk systems and governance structures, internal auditors do not need to answer the question of where financial regulation — and other risks — "go from here." Instead, internal auditors need to figure out more effective and efficient ways to continuously ask the right questions.

ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Cory Gunderson
Managing Director, Global Leader
Financial Services Industry
+1.212.708.6313
cory.gunderson@protiviti.com

Michael Thor
Managing Director, North American Leader
Internal Audit and Financial Advisory for the
Financial Services Industry
+1.317.510.4685
mike.thor@protiviti.com

Charlie Anderson
Managing Director, Data Management
and Advanced Analytics
+1.312.364.4922
charlie.anderson@protiviti.com

Ed Page
Managing Director,
Technology Consulting
+1.312.476.6093
ed.page@protiviti.com

Shaheen Dil
Managing Director, Global Leader
Data Management and Advanced Analytics
+1.212.603.8378
shaheen.dil@protiviti.com

Barbi Goldstein
Managing Director, Internal Audit
and Financial Advisory
+1.212.603.8351
barbi.goldstein@protiviti.com

James Armetta
Managing Director, Internal Audit
and Financial Advisory
+1.212.399.8606
james.armetta@protiviti.com

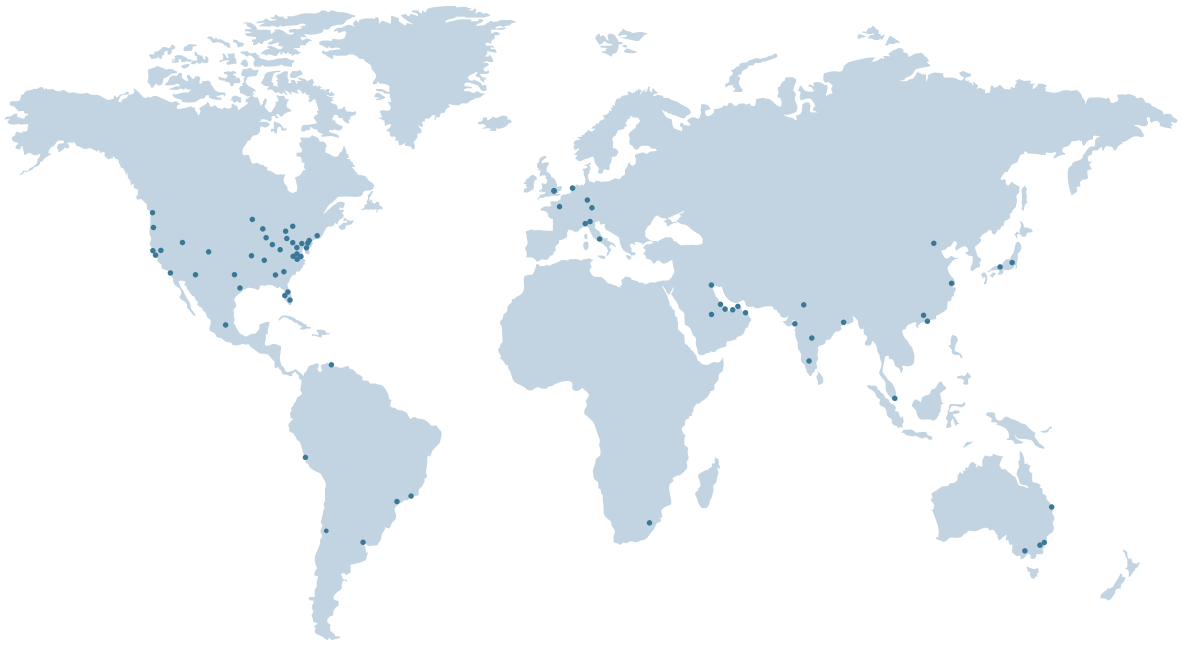
Matthew Perconte
Managing Director,
Risk and Compliance
+1.312.476.6998
matthew.perconte@protiviti.com

Matthew Moore
Managing Director, Global Leader
Risk and Compliance
+1.704.972.9615
matthew.moore@protiviti.com

Scott Jones
Managing Director, Internal Audit
and Financial Advisory
+1.213.327.1442
scott.jones@protiviti.com

James McDonald
Managing Director,
Risk and Compliance
+1.704.998.0786
james.mcdonald@protiviti.com

Jason Goldberg
Director,
Business Performance Improvement
+1.212.471.9678
jason.goldberg@protiviti.com



THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Indianapolis
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE*
Santiago

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE MIDDLE EAST AFRICA

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

UNITED KINGDOM
London

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

SOUTH AFRICA*
Johannesburg

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM

protiviti®