Priorities for Internal Auditors in U.S. Healthcare Provider Organizations

Chief Concerns Include Cybersecurity, Regulatory Compliance and Fraud

ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Risk & Business Consulting.
Internal Audit.

INTRODUCTION

Technology is a double-edged sword.

From an IT perspective, the healthcare industry has plunged into a new age. There has never been a greater emphasis on the implementation of, and reliance on, transformative new technologies that are delivering promising breakthroughs in patient care, operating efficiencies and organizational performance. Sensitive healthcare data is being accessed and used in numerous new ways.

This change is fueling historic innovation. At the same time, it is exposing healthcare organizations to new challenges and risks. Chief among these is cybersecurity.

While healthcare internal audit functions absolutely need to address cybersecurity issues, they must do so while juggling many other priorities whose number and nature continue to shift due to the ongoing digital transformation, new regulatory requirements and a volatile marketplace.

The results of the **2015 Internal Audit Capabilities and Needs Survey of Healthcare Provider Organizations** from AHIA and Protiviti shed light on the ways in which chief audit executives (CAEs) and internal audit professionals are performing this strategic juggling act while providing assurance across an ever-increasing number of risk areas. Our results indicate that the most important of these competing priorities include health information exchanges, health insurance exchanges, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, and multiple aspects of fraud prevention.

Further, our results show that healthcare internal audit functions are focusing their attention and resources in five key areas of priority, which we discuss further in our report:

1. Cybersecurity risks and practices
2. Regulatory compliance
3. Supporting, enabling and protecting the digital enterprise
4. Addressing fraud risks
5. Multi-stakeholder collaboration

About the Survey

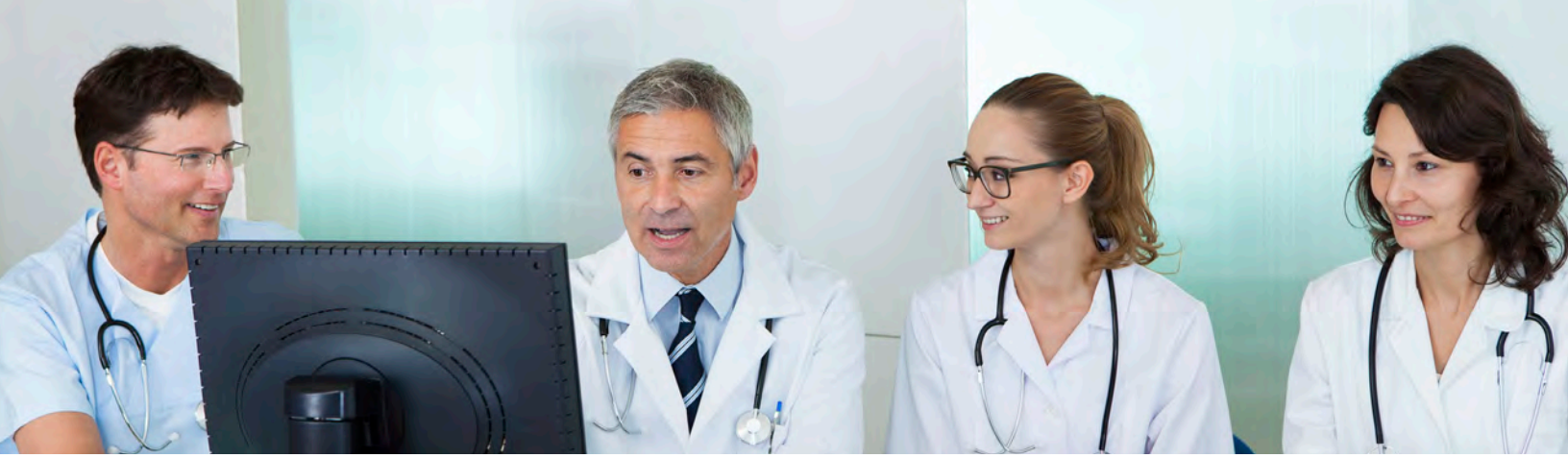
Protiviti conducts its Internal Audit Capabilities and Needs Survey annually to assess current skill levels of internal audit executives and professionals, identify areas in need of improvement and help stimulate the sharing of leading practices throughout the profession. This year, survey respondents answered close to 150 questions in the study's three standard categories: General Technical Knowledge, Audit Process Knowledge, and Personal Skills and Capabilities.

In each category, respondents were asked to assess, on a scale of one to five, their competency in the different skills and areas of knowledge, with "1" being the lowest level of competency and "5" being the highest. They were then asked to indicate whether they believe they possess an adequate level of competency or if there is need for improvement, taking into account the circumstances of their organization and the nature of the industry.

Respondents also answered a separate set of questions in a special section, "Cybersecurity and the Audit Process."

The overall results, which are based on information provided by all respondents (who numbered more than 800), are contained within the master report (available at www.protiviti.com/IAsurvey).

Respondents from healthcare providers – who comprise 6 percent (n=48) of the survey participants – also answered questions in a unique section featuring internal audit areas specific to the healthcare industry. AHIA and Protiviti partnered to analyze these results and produce this report in order to equip internal audit executives and professionals in the healthcare industry with more targeted insights about the unique challenges within their domains.



CYBERSECURITY RISKS AND PRACTICES

The magnitude, frequency and cost of cybersecurity incidents are increasing dramatically in a multitude of industries. Healthcare provider organizations are well-aware of this troubling trend, particularly given the recent cyberattacks that many in the industry have experienced in recent months. The fact is attempted breaches seem all but guaranteed to escalate for healthcare provider organizations, in great part because of the high value criminals place on stolen healthcare data.

These risks are exacerbated by the growing number of third-party vendors that have access to healthcare data – at least some of which may have gaps in their data security. Vendor risk management remains a top-of-mind concern. Furthermore, with multiple hospitals and Accountable Care Organizations (ACOs) accessing the same electronic health records (EHR) systems for patient data and statistics, the potential for cybersecurity incidents increases.

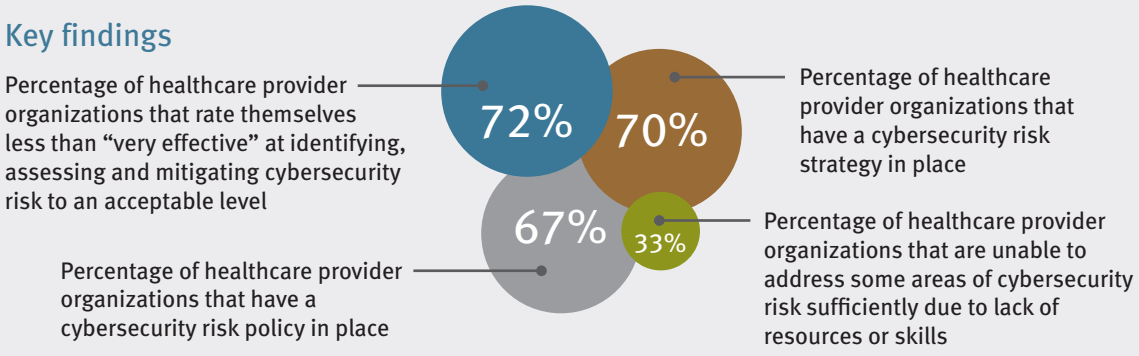
In this year's survey, we included a special section to assess the current state of cybersecurity risk in healthcare provider organizations. Our results indicate internal audit functions view strengthening data security, adhering to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, and mastering new data analysis and auditing technology to be among their highest priorities (these key points also are evident in other sections of the survey).

Specifically, our results show:

- High confidence is generally lacking among internal audit leaders and professionals in current cybersecurity capabilities of healthcare provider organizations, including identifying, assessing and mitigating cybersecurity risk to an acceptable level.
- Senior management's level of awareness regarding information security exposures is an area for improvement.
- On average, one in three healthcare provider organizations lack a cybersecurity risk strategy as well as a cybersecurity risk policy.
- On the positive side, a strong majority of healthcare provider organizations address cybersecurity risk in their risk assessment.

Ten Cybersecurity Action Items for CAEs and Internal Audit
1. Work with management and the board to develop a cybersecurity strategy and policy.
2. Seek to have the organization achieve a high level of effectiveness in its ability to identify, assess and mitigate cybersecurity risk to an acceptable level.
3. Recognize the threat of a cybersecurity breach resulting from the actions of an employee or business partner.
4. Leverage board relationships to (a) heighten the board's awareness and knowledge of cybersecurity risk; and (b) ensure that the board remains highly engaged with cybersecurity matters and up to date on the changing nature and strategic importance of cybersecurity risk.
5. Ensure cybersecurity risk is formally integrated into the audit plan.
6. Develop, and keep current, an understanding of how emerging technologies and technological trends are affecting the company and its cybersecurity risk profile.
7. Evaluate the organization's cybersecurity program against the NIST Cybersecurity Framework, while recognizing that the framework does not go to the control level and therefore may require additional evaluations of ISO 27001 and 27002.
8. Recognize that with regard to cybersecurity, the strongest preventative capability requires a combination of human and technology security – a complementary blend of education, awareness, vigilance and technology tools.
9. Reinforce the need for cybersecurity monitoring and cyber-incident response with management – a clear escalation protocol can help make the case for (and sustain) this priority.
10. Highlight any IT/audit staffing and resource shortages, which represent a top technology challenge in many organizations and can hamper efforts to address cybersecurity issues.

Key findings



REGULATORY COMPLIANCE

Addressing regulatory compliance remains a critical mandate in the healthcare industry, with federal, state and industry regulations ever-changing and increasingly burdensome. Our survey shows that chief audit executives and their teams are committed to strengthening their knowledge and expertise of new and emerging regulatory compliance requirements, many of which are provisions of the Patient Protection and Affordable Care Act (PPACA).

Similar to last year's results, understanding health information exchanges ranks among the top priorities for healthcare internal audit functions, as does a new area to this year's study, health insurance exchanges. Of particular note, both health information exchanges and health insurance exchanges received relatively low competency ratings (1.9 and 1.7, respectively, on a 5-point scale), suggesting there are major improvement opportunities in these areas.

Table 1: Healthcare Industry-Specific Technical Knowledge – Overall Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1 (tie)	Health information exchanges	1.9
	Health insurance exchanges	1.7
2 (tie)	Accountable care organizations	2.6
	Patient Protection and Affordable Care Act provisions	2.1
	State-specific prompt payment laws	2.0
3 (tie)	Accreditation environment (e.g., The Joint Commission)	2.6
	Ancillary services (pharmacy, lab, radiology, etc.)	2.4
	Cash acceleration programs	2.0
	Fraud investigations	2.7
	Healthcare joint ventures	2.1
	Hospice	1.9
	ICD-10 impact, readiness and implementation	2.4
	Medicare cost reporting	2.2
	Hospital value-based purchasing	2.1
	Physician compensation methodologies (e.g., wRVU)	2.1
	Professional fee billing	1.9
	Provider contracting	2.2
	Reimbursement methodologies (Medicare, Medicaid, etc.)	2.3

While many PPACA implementation objectives have been achieved (e.g., providing access to insurance for uninsured Americans with pre-existing conditions, prescription drug discounts for seniors and allowing providers to organize as ACOs), significant compliance challenges remain. Organizations are just now coming to realize and understand what operating an ACO really means. Internal audit needs to ramp up its knowledge base to serve effectively as an assurance function.

PPACA provisions comprise a major portion of regulatory compliance activities. However, healthcare organizations also must contend with many other compliance-related issues, including but not limited to ICD-10, Medicare cost reporting and fraud investigations.

Table 2: Healthcare Industry-Specific Technical Knowledge – CAE Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1 (tie)	Cost reporting	2.1
	Health information exchanges	1.9
	Health insurance exchanges	1.7
	Medicare cost reporting	2.2
	Hospital value-based purchasing	2.1
	Reimbursement methodologies (Medicare, Medicaid, etc.)	2.3
	State-specific prompt payment laws	2.0
	Accountable care organizations	2.6

Table 3: Healthcare Industry-Specific Technical Knowledge – Overall Results, Three-Year Comparison

2015	2014	2013
Health information exchanges	Health information exchanges	Health information exchanges
Health insurance exchanges	eDiscovery	Value-based purchasing
Accountable care organizations	Meaningful Use compliance	ICD-10 implementation
Patient Protection and Affordable Care Act provisions	Coding knowledge (ICD-9, ICD-10, HCC, HCPCS, CPT)	Payment bundling
State-specific prompt payment laws	Healthcare joint ventures	Accountable care organizations
Accreditation environment (e.g., The Joint Commission)	Physician compensation methodologies (e.g., wRVU)	Clinical documentation
Ancillary services (pharmacy, lab, radiology, etc.)	Risk pool/capitation accounting	ICD-10 impact and readiness
Cash acceleration programs	Cost containment – labor and non-labor	Pay-for-performance quality standards (CMS core measures and HCAHPS)
Fraud investigations	Delivery System Reform Incentive Payment (DSRIP) program	State-specific privacy/security laws
Healthcare joint ventures	Hospital value-based purchasing	
Hospice	ICD-10 impact, readiness and implementation	
ICD-10 impact, readiness and implementation	Medicare Modernization Act	
Medicare cost reporting	State-specific prompt payment laws	
Hospital value-based purchasing	State-specific privacy/security laws	
Physician compensation methodologies (e.g., wRVU)		
Professional fee billing		
Provider contracting		
Reimbursement methodologies (Medicare, Medicaid, etc.)		

= Three-year trend

Table 4: Healthcare Industry-Specific Technical Knowledge – CAE Results, Three-Year Comparison

2015	2014	2013
Cost reporting	Health information exchanges	Health information exchanges
Health information exchanges	IRB and clinical trials	Payment bundling
Health insurance exchanges	Meaningful Use compliance	ICD-10 implementation
Medicare cost reporting	Physician compensation methodologies (e.g. wRVU)	Pay-for-performance quality standards (CMS core measures and HCAHPS)
Hospital value-based purchasing	Case management	Physician credentialing
Reimbursement methodologies (Medicare, Medicaid, etc.)	Coding knowledge (ICD-9, ICD-10, HCC, HCPCS, CPT)	Value-based purchasing
State-specific prompt payment laws	Delivery System Reform Incentive Payment (DSRIP) program	Durable medical equipment
Accountable care organizations	eDiscovery	eDiscovery
	Healthcare joint ventures	HIPAA 5010
	Pandemic planning/business continuity	Physician alignment and employment strategies
	Physician organizations	Physician organizations
	Risk pool/capitation accounting	Professional fee billing
		Quality of care

= Three-year trend

Key finding

7.5

Senior management's level of awareness with regard to the organization's information security exposures (1-10 scale where "10" indicates high level of awareness)

Key finding

6.7

Level of confidence that the organization is able to prevent an opportunistic breach as a result of actions by an insider (1-10 scale, where "10" indicates high level of confidence)

SUPPORTING, ENABLING AND PROTECTING THE DIGITAL ENTERPRISE

Technology – and the many ways in which it increasingly is transforming healthcare providers into digital enterprises – remains the topic du jour for healthcare internal auditors. Within the technology area, cybersecurity clearly marks a major concern. And it very much should, given the rising instances of cybersecurity breaches in the industry.

Our results show that the NIST Cybersecurity Framework represents a top priority for internal audit. Healthcare internal audit leaders and professionals also view strengthening data security, mastering new data analysis and addressing other IT risks (including those related to the rapid spread of social and mobile applications) among their top priorities.

Table 5: General Technical Knowledge – Overall Healthcare Industry Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	NIST Cybersecurity Framework	2.5
2 (tie)	ISO 14000 (environmental management)	1.9
	Reporting on Controls at a Service Organization – SSAE 16/AU 324 (replaces SAS 70)	2.6
3 (tie)	ISO 9000 (quality management and quality assurance)	2.1
	GTAG 16 – Data Analysis Technologies	2.6
	The Guide to the Assessment of IT Risk (GAIT)	2.3
	ISO 27000 (information security)	1.9
	Social media applications	3.1
	Mobile applications	2.6

It is no surprise that the NIST Cybersecurity Framework, which was finalized in 2014, is a priority, particularly as new cybersecurity legislative proposals are weighed by Congress in the wake of high-profile cybersecurity incidents. Cybersecurity, however, is far from the only technology-related issue affecting healthcare companies. In fact, two out of three healthcare organizations continue to work through "major IT transformations."[1]

This transformation toward a more digital enterprise is particularly complex within the healthcare industry because it introduces to a heavily regulated environment new and disruptive technologies that are changing the way healthcare organizations operate. Healthcare internal audit departments and their organizations are working to adapt their risk management capabilities to address an increasingly digital enterprise amid so many challenges – including the introduction of health information exchanges and health insurance exchanges, constant regulatory uncertainty, HIPAA compliance audits, social media misuse, increased fraud activity and regulations, recoupment of Meaningful Use funds, ICD-10 changes, and much more.

[1] According to healthcare industry respondents in Protiviti's 2015 IT Priorities Survey: www.protiviti.com/ITpriorities.

Our findings also indicate internal auditors are committed to fortifying IT and data risk management, strengthening overall IT risk management capabilities, and keeping close tabs on emerging technologies and emerging risks. Part of this work includes gaining knowledge of relevant ISO standards, including ISO 14000 and ISO 27000.

One last note regarding cybersecurity: As health information exchanges and health insurance exchanges mature, the need to keep data secure, accurate and private will only increase, especially as this data is shared more frequently with more external partners.

Table 6: General Technical Knowledge – CAE Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1 (tie)	NIST Cybersecurity Framework	2.7
	Mobile applications	2.6
	The Guide to the Assessment of IT Risk (GAIT)	2.3
	Social media applications	2.9
2 (tie)	2013 COSO Internal Control Framework – Evaluation of "Present, Functioning and Operating Together"	2.9
	ISO 14000 (environmental management)	1.8
	Reporting on Controls at a Service Organization – SSAE 16 / AU 324 (replaces SAS 70)	2.5
	2013 COSO Internal Control Framework – Information and Communication	3.0

Table 7: General Technical Knowledge – Overall Results, Three-Year Comparison

2015	2014	2013
NIST Cybersecurity Framework	Recently enacted IIA Standard: Overall Opinions (Standard 2450)	Cloud computing
ISO 14000 (environmental management)	Social media applications	GTAG 16 – Data analysis technologies
Reporting on Controls at a Service Organization – SSAE 16/AU 324 (replaces SAS 70)	Mobile applications	ISO 27000 (information security)
ISO 9000 (quality management and quality assurance)	Recently enacted IIA Standards: Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)	GTAG 17 – Auditing IT governance
GTAG 16 – Data Analysis Technologies	GTAG 16 – Data Analysis Technologies	Social media applications
The Guide to the Assessment of IT Risk (GAIT)	NIST Cybersecurity Framework	Fraud risk management
ISO 27000 (information security)	GTAG 6 – Managing and Auditing IT Vulnerabilities	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)
Social media applications	GTAG 15 – Information Security Governance	IT governance
Mobile applications	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)	
	GTAG 10 – Business Continuity Management	
	ISO 27000 (information security)	
	Reporting on Controls at a Service Organization – SSAE 16/AU 324 (replaces SAS 70)	

= Three-year trend

Table 8: General Technical Knowledge – CAE Results, Three-Year Comparison

2015	2014	2013
NIST Cybersecurity Framework	Mobile applications	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)
Mobile applications	NIST Cybersecurity Framework	Social media applications
The Guide to the Assessment of IT Risk (GAIT)	Social media applications	COSO Internal Control Framework
Social media applications	Cloud computing	Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)
2013 COSO Internal Control Framework – Evaluation of "Present, Functioning and Operating Together"	ISO 27000 (information security)	GTAG 6 – Managing and Auditing IT Vulnerabilities
ISO 14000 (environmental management)	GTAG 6 – Managing and Auditing IT Vulnerabilities	GTAG 17 – Auditing IT Governance
Reporting on Controls at a Service Organization – SSAE 16 / AU 324 (replaces SAS 70)	GTAG 15 – Information Security Governance	ISO 27000 (information security)
2013 COSO Internal Control Framework – Information and Communication		

= Three-year trend

More on the NIST Cybersecurity Framework

When it comes to assessing the strength of current cybersecurity measures, the NIST Cybersecurity Framework can serve as a useful litmus test for organizations and internal audit functions. Many qualities of this framework also describe key aspects of leading practices within internal audit: It is risk-based, it is complementary with other risk programs, and it is subject to change and enhancement. However, technically NIST compliance is voluntary in the regulatory sense (yet all but required from a governance perspective).

More internal audit functions are discovering that the NIST framework's approach mirrors their existing program assessments:

1. Define the business priorities and the scope of the [cybersecurity] program.
2. Define the assets in scope and the threats to them.
3. Create an "As Is" or baseline profile of the organization's security program implementation.
4. Perform a risk assessment of the organization's readiness.
5. Create a "To Be" statement/objective for the security program.
6. Define gaps between the "As Is" and "To Be" states, assess their impact and prioritize remediation activities.

With regard to the last point, these gaps are, of course, crucial. Internal auditors witness this type of gap when realizing that the NIST framework is incomplete, in that it does not reach the control level, where ISO 27000 (information security) standards can be applied. Savvy internal auditors are adept at filling a wide range of risk-management and knowledge gaps. That helps explain why ISO 27000 (information security) ranks among the top 10 priorities for internal auditors this year.

ADDRESSING FRAUD RISKS

The financial figures related to the largest instance of suspected Medicare fraud, as reported by federal officials last June, are staggering: $712 million in false billing, criminal charges filed against 243 individuals, $263 million in different fraud schemes in greater Miami alone, and $23 million in fraudulent billing by a single Los Angeles doctor.[2] These numbers suggest the federal government may easily surpass the more than $3.3 billion it recovered in fiscal 2014 from individuals and organizations that attempted to defraud federal health programs.

Given this environment of extensive fraud against government healthcare programs, combined with the ever-present risk of occupational fraud, it's not surprising to find fraud issues among the top priorities for healthcare internal auditors. Fraud risk assessment, fraud risk, fraud monitoring and fraud auditing make up four of their six top areas of focus as identified in the Audit Process Knowledge category of our survey.

The FBI recently reported it is currently investigating a staggering 2,700 instances of potential healthcare fraud. Thus, it is likely fraud will remain a critical priority for healthcare internal audit departments.

Table 9: Audit Process Knowledge – Overall Healthcare Industry Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Fraud – fraud risk assessment	2.9
2 (tie)	Fraud – fraud risk	3.1
	Fraud – monitoring	2.9
3 (tie)	Auditing IT – security	2.4
	Continuous auditing	2.8
	Fraud – auditing	3.4
4	Assessing risk – emerging issues	3.0

Table 10: Audit Process Knowledge – CAE Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Auditing IT – security	2.2
2 (tie)	Computer-assisted audit tools (CAATs)	2.8
	Data analysis tools – data manipulation	2.8
	Continuous auditing	3.0
	Data analysis tools – statistical analysis	2.6
	Marketing internal audit internally	3.6
	Fraud – monitoring	3.4
	Continuous monitoring	3.0

[2] Barrett, Devlin, "Feds Charge More Than 200 People With Medicare Fraud," *The Wall Street Journal*, June 18, 2015: www.wsj.com/articles/feds-charge-more-than-200-people-with-medicare-fraud-1434641497?cb=logged0.30454330751562186.

Table 11: Audit Process Knowledge – Overall Results, Three-Year Comparison

2015	2014	2013
Fraud – fraud risk assessment	Quality Assurance and Improvement Program (IIA Standard 1300) – Periodic Reviews (IIA Standard 1311)	Data analysis tools – data manipulation
Fraud – fraud risk	Statistically based sampling	Quality assurance and improvement program (IIA Standard 1300) – External assessment (IIA Standard 1312)
Fraud – monitoring	Auditing IT – new technologies	Quality assurance and improvement program (IIA Standard 1300) – Ongoing reviews (IIA Standard 1311)
Auditing IT – security	Marketing internal audit internally	Quality assurance and improvement program (IIA Standard 1300) – Periodic reviews (IIA Standard 1311)
Continuous auditing	Auditing IT – program development	Fraud – fraud risk assessment
Fraud – auditing	Auditing IT – security	Enterprisewide risk management
Assessing risk – emerging issues	CAATs	Fraud – monitoring
	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (Standard 1312)	Assessing risk – emerging issues
	Assessing risk – emerging issues	

= Three-year trend

Table 12: Audit Process Knowledge – CAE Results, Three-Year Comparison

2015	2014	2013
Auditing IT – security	Auditing IT – new technologies	Auditing IT – new technologies
Computer-assisted audit tools (CAATs)	Auditing IT – security	Quality assurance and improvement program (IIA Standard 1300) – External assessment (IIA Standard 1312)
Data analysis tools – data manipulation	Marketing internal audit internally	Quality assurance and improvement program (IIA Standard 1300) – Ongoing reviews (IIA Standard 1311)
Continuous auditing	Assessing risk – emerging issues	Quality assurance and improvement program (IIA Standard 1300) – Periodic reviews (IIA Standard 1311)
Data analysis tools – statistical analysis	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (Standard 1312)	Enterprisewide risk management
Marketing internal audit internally	Quality Assurance and Improvement Program (IIA Standard 1300) – Periodic Reviews (IIA Standard 1311)	Auditing IT – security
Fraud – monitoring	Statistically based sampling	Data analysis tools – data manipulation
Continuous monitoring		Presenting to the audit committee

= Three-year trend

MULTI-STAKEHOLDER COLLABORATION

As this report's preceding sections demonstrate, healthcare internal audit functions confront a formidable set of challenges. While these issues vary significantly – ranging from cybersecurity to health insurance exchanges to digital transformation and more – they share a common attribute: complexity. Cybersecurity and overall IT risk management, for example, require cooperation among colleagues in IT, risk management, operations, legal counsel and other departments. Effectively addressing these multidimensional challenges requires internal auditors to work across a number of different internal functions and, often, with a number of external parties.

This work boils down to persuading business partners throughout the organization to integrate risk considerations into every decision they make. This effort is evident in our survey results, where high-pressure meetings and persuasion represent the top priorities within the personal skills and capabilities category (see Tables 13 and 14).

Other highly ranked priorities – presenting (small groups) and negotiation – point to internal audit's drive to collaborate with different stakeholders, including senior executives, board committees and outside networks.

Table 13: Personal Skills and Capabilities – Overall Healthcare Industry Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1 (tie)	High-pressure meetings	3.1
	Persuasion	3.1
2 (tie)	Negotiation	2.8
	Presenting (small groups)	2.9
3 (tie)	Developing other board committee relationships	2.8
	Developing outside contacts/networking	3.5
	Developing rapport with senior executives	3.2
	Leadership (within the internal audit profession)	3.1
	Presenting (public speaking)	3.1
	Strategic thinking	3.2
	Using/mastering new technology and applications	3.1

The ability to collaborate effectively with multiple stakeholders is a key enabler of internal audit's ongoing drive to contribute value by:

- Thinking more strategically when analyzing risk and framing audit plans;
- Providing early warning and education on new and emerging risks;
- Broadening focus on operations, compliance and nonfinancial reporting issues;
- Strengthening the lines of defense that make risk management work; and
- Improving the information for decision-making across the organization.[3]

Two priorities, developing other board committee relationships and negotiation, are noteworthy for the relatively low competency ratings (a 2.8 on a 5-point scale) among our respondents.

The personal skills priority lists for all respondents, including CAEs, are lengthy. Overall, respondents identified 11 nearly equally important priorities that point to an underlying desire to enhance the value internal audit delivers to the organization – even in the face of new multi-dimensional challenges.

Table 14: Personal Skills and Capabilities – CAE Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Persuasion	3.8
2 (tie)	Strategic thinking	3.6
	Presenting (small groups)	3.8
	Developing outside contacts/networking	4.2
	High-pressure meetings	4.0
3 (tie)	Using/mastering new technology and applications	3.4
	Negotiation	3.8
	Creating a learning internal audit function	3.6
	Presenting (public speaking)	3.8

[3] A more comprehensive discussion of these activities is available in *The Bulletin*, Volume 5, Issue 6, "The Future Auditor: The Chief Audit Executive's Endgame," available at www.protiviti.com.

Table 15: Personal Skills and Capabilities – Overall Results, Three-Year Comparison

2015	2014	2013
High-pressure meetings	Presenting (public speaking)	Presenting (public speaking)
Persuasion	Developing other board committee relationships	High-pressure meetings
Negotiation	Developing outside contacts/networking	Dealing with confrontation
Presenting (small groups)	Leadership (within your organization)	Persuasion
Developing other board committee relationships	Persuasion	Using/mastering new technology and applications
Developing outside contacts/networking	Time management	
Developing rapport with senior executives	Using/mastering new technology and applications	
Leadership (within the internal audit profession)	Dealing with confrontation	
Presenting (public speaking)	Developing audit committee relationships	
Strategic thinking	Negotiation	
Using/mastering new technology and applications		

= Three-year trend

Table 16: Personal Skills and Capabilities – CAE Results, Three-Year Comparison

2015	2014	2013
Persuasion	Using/mastering new technology and applications	Coaching/mentoring
Strategic thinking	Developing audit committee relationships	Negotiation
Presenting (small groups)	Developing other board committee relationships	High-pressure meetings
Developing outside contacts/networking	Developing outside contacts/networking	Dealing with confrontation
High-pressure meetings	Negotiation	Presenting (public speaking)
Using/mastering new technology and applications	Presenting (public speaking)	Persuasion
Negotiation	High-pressure meetings	Strategic thinking
Creating a learning internal audit function	Persuasion	Using/mastering new technology and applications
Presenting (public speaking)		Developing audit committee relationships

= Three-year trend

CLOSING THOUGHTS

Healthcare internal audit leaders and professionals continue to demonstrate a commitment to professional growth and development in the face of growing challenges in the industry. An increasing portion of this work is designed to reduce the risks that new and emerging technology can create, which in turn helps optimize the value that healthcare provider organizations derive from the increasingly innovative and promising benefits that this technology delivers. As healthcare provider organizations continue their digital transformations, this internal audit work will become more important, and ever more valuable.

For additional information and insights, we invite you to review the following resources from AHIA and Protiviti:

AHIA (www.ahia.org)

Third-Party Relationships and Your Confidential Data

HHS/OIG "Practical Guidance for Health Care Governing Boards on Compliance Oversight"

Protiviti (www.protiviti.com)

From Cybersecurity to Collaboration: Assessing the Top Priorities for Internal Audit Functions

HIPAA Security – Prepare Now or 'Wait and See'?

A Global Look at IT Audit Best Practices

mHealth: How Mobile Apps Can Help Health Plans Improve Consumer Engagement and Facilitate Behavior Change

2015 Vendor Risk Management Benchmark Study

ABOUT AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network.

Contact

Todd Havens
AHIA White Paper Committee Chair
+1.484.884.1406
todd.havens@lvhn.org

ABOUT PROTIVITI

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, 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

Brian Christensen
Executive Vice President – Global Internal Audit
+1.602.273.8020
brian.christensen@protiviti.com

Susan Haseley
Managing Director – Healthcare Industry Leader
+1.469.374.2435
susan.haseley@protiviti.com

ahia
Assoc. of Healthcare Internal Auditors

Education – Networking – Resources

protiviti®
Risk & Business Consulting.
Internal Audit.

www.protiviti.com

PRO-0815-103069