Cybersecurity, IT Transformation and Analytics – Addressing Priorities for Internal Auditors in U.S. Healthcare Provider Organizations

ahia
Assoc. of Healthcare Internal Auditors

protiviti®
Risk & Business Consulting.
Internal Audit.

CONTENTS

1. How Is Your Healthcare Organization's Internal Audit Function Evolving? . . . 1
2. Cybersecurity and the Audit Process . . . 3
3. Electronic Health Records, Information Technology Transformation and Digitization . . . 7
4. Technology-Enabled Auditing and Managing Fraud Risk . . . 11
5. Collaboration and Communication Between Internal Audit and the Organization . . . 14
6. Closing Thoughts . . . 17
7. About AHIA . . . 18
8. About Protiviti . . . 18

HOW IS YOUR HEALTHCARE ORGANIZATION'S INTERNAL AUDIT FUNCTION EVOLVING?

Healthcare providers are still in the process of converting hard-copy patient files to electronic records. They are exchanging and analyzing more sensitive information in digital form, making it portable and creating a single source of truth accessible via a wide range of mobile devices and through cloud-based third-party service organizations. Life-saving devices – such as pacemakers and infusion pumps, among many others – are increasingly networked and vulnerable to cyberattack, adding patient health risk as another new dimension to previous concerns regarding the protection of health information.

The digitization of the healthcare industry is a transformation on par with the sweeping changes in financial services over the past 20 years. Internal audit functions with healthcare providers are expected not only to keep up with these changes and the associated risks, but also to look ahead and help management and the board identify emerging risks on the horizon.

For the past 10 years, Protiviti has surveyed chief audit executives and internal audit leaders and practitioners across a broad spectrum of industries to document the state of the internal audit profession and the drivers of change. This year, we again partnered with the Association of Healthcare Internal Auditors to glean more targeted insights regarding the industry's unique internal audit challenges. The results of the 2016 Internal Audit Capabilities and Needs Survey of Healthcare Provider Organizations provide a benchmark of current perceptions in the industry, as well as an indication of what internal audit leaders will need to help their organizations face the future with confidence.

Our results show that healthcare internal audit functions view priorities in four key areas, which we review in our report:

1. Cybersecurity and the audit process
2. Electronic health records, information technology transformation and digitization
3. Technology-enabled auditing and managing fraud risk
4. Collaboration and communication between internal audit and the organization

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 1,300), are contained within the master report (available at www.protiviti.com/IAsurvey).

Respondents from healthcare providers – who comprise 8 percent of the survey participants – also answered questions in a unique section featuring internal audit areas specific to healthcare providers. AHIA and Protiviti partnered to analyze these results and publish this paper in order to equip internal audit executives and professionals in healthcare provider organizations with more targeted insights about the unique challenges within their domains.

CYBERSECURITY AND THE AUDIT PROCESS

Medical records contain a wealth of information that can be used for identity theft and fraud (such as social security number, address or claims data). Personal health information, in fact, carries a higher value on the black market than credit card data. Indeed, while a credit card record might fetch $2 on the black market, a medical record can average more than $20, according to a June 2015 report by the Workgroup for Electronic Data Interchange (WEDI), a nonprofit association for users of electronic data interchange in healthcare.[1]

The value of personal healthcare information is greater not only because of the data, but also because identity theft is more difficult to detect and mitigate in healthcare. Unlike a credit card that can be easily canceled in minutes and replaced in hours, there is no easy way to repair the integrity of healthcare records once they have been breached, nor for an individual whose information is compromised to "cancel" or invalidate that data. As a result, the frequency, scope and sophistication of cyberattacks in the healthcare industry are growing at a worrisome rate. According to WEDI, data breaches for healthcare organizations in the first four months of 2015 alone were almost three times the total for the previous four years combined.

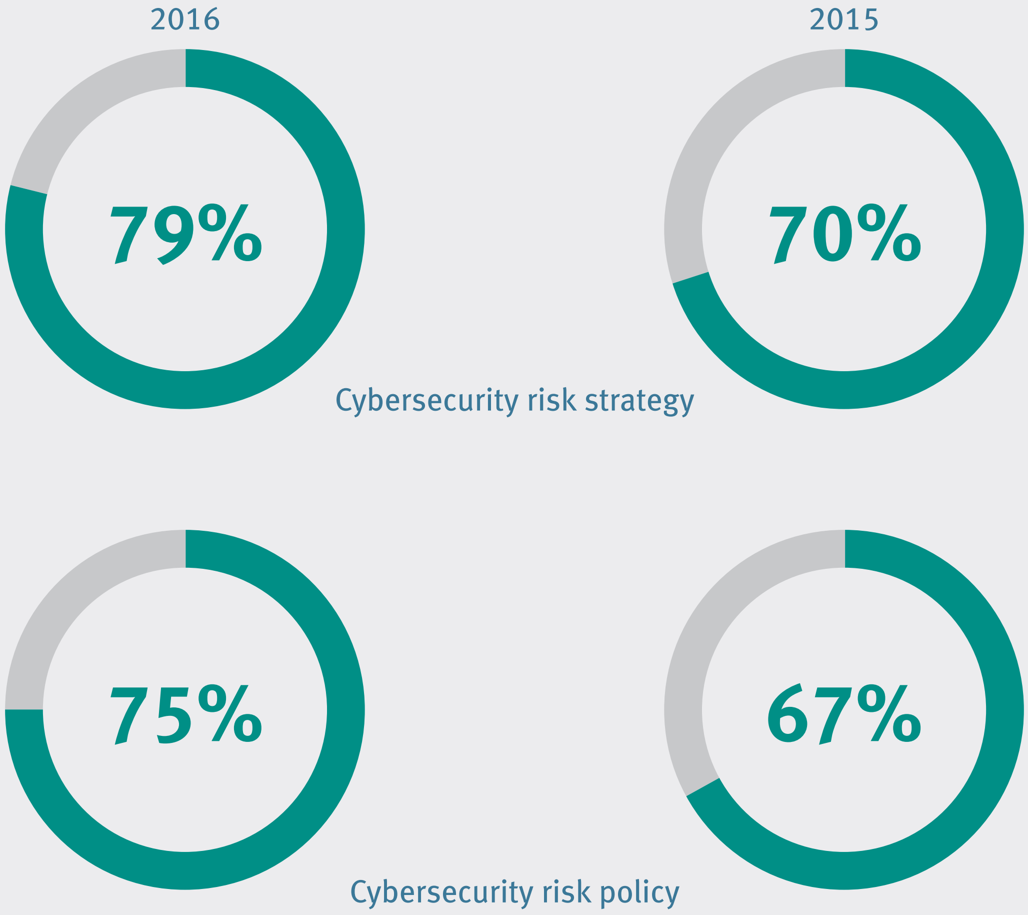
And while healthcare organizations have made great progress in leveraging IT to drive improvements in quality and efficiency of patient care, our survey data suggests they may lack the internal audit resources to effectively detect, mitigate and prevent cyberthreats.

Specifically, our survey results show:

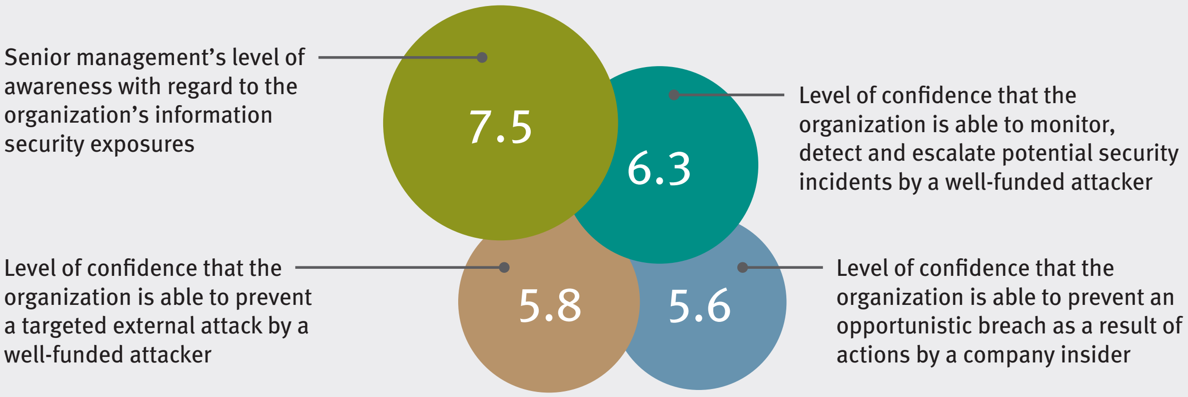
- Senior management is highly aware of the organization's cybersecurity risks. This is a good first step toward addressing the challenge.
- However, there is only moderate confidence in the ability of healthcare provider organizations to protect sensitive information from internal or external attack.
- Despite the critical and growing importance of information security, a plurality of survey respondents indicated their boards possessed only a moderate understanding of this existential threat.
- A majority of organizations are unable to address some aspects of cybersecurity risk due to a lack of resources – significantly more compared to our 2015 survey results.

[1] WEDI, Perspectives on Cybersecurity in Healthcare, June 2015, www.wedi.org/docs/test/cyber-security-primer.pdf?sfvrsn=0.

Healthcare provider organizations with a cybersecurity risk strategy and policy in place

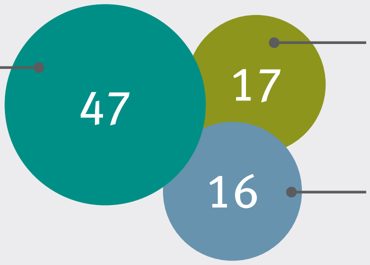


Key Findings (ratings based on a scale of 1-10)



Key Findings

Percentage of healthcare providers that have received inquiries from customers/clients or insurance providers about the organization's state of cybersecurity

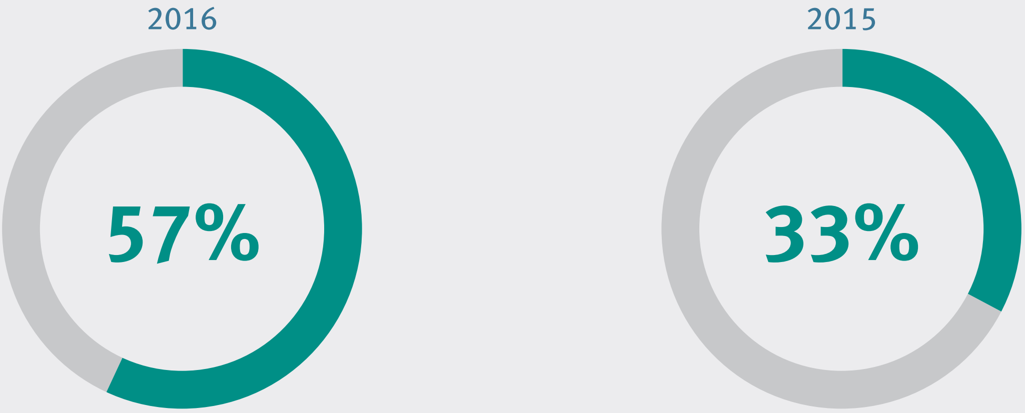


Percentage of healthcare providers that do not address cybersecurity risk in their risk assessments

Percentage of healthcare providers that have no plans to evaluate and audit cybersecurity risk as part of the annual audit plan

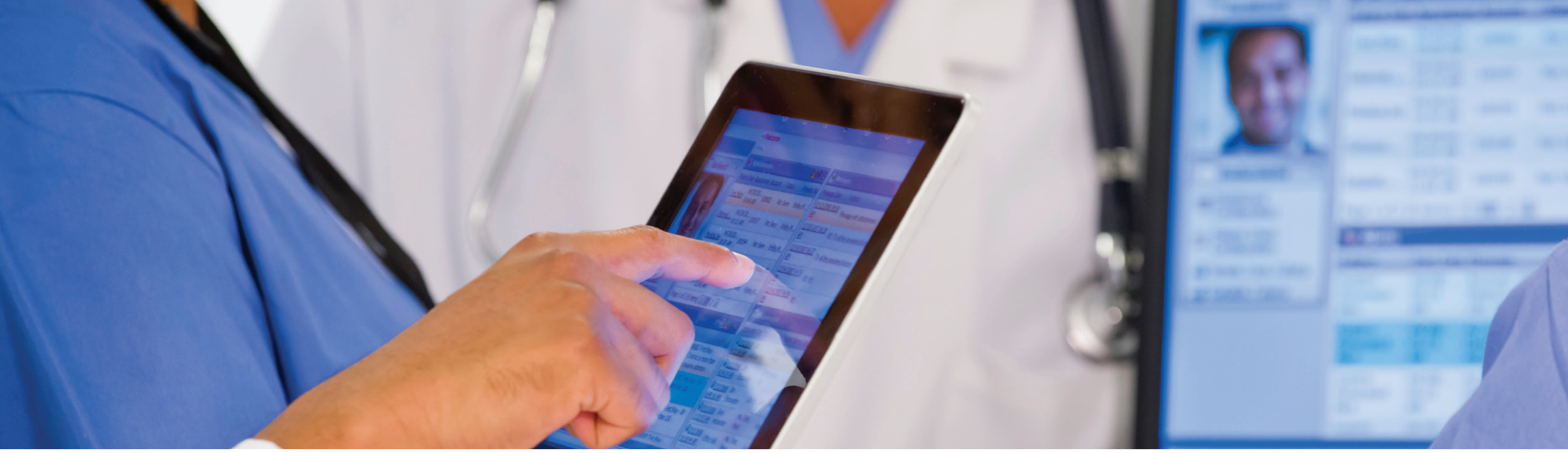
Are there specific areas of cybersecurity risk that you are not able to address sufficiently in your audit plan due to a lack of resources or skills?

Shown: "Yes" responses



Ten Cybersecurity Action Items for Chief Audit Executives and Internal Audit

1. Work with management and the board to develop a cybersecurity strategy and policy.
2. Identify and act on opportunities to improve the organization’s ability to identify, assess and mitigate cybersecurity risk to an acceptable level.
3. Recognize that cybersecurity risk is not only external – assess and mitigate potential threats that could result from the actions of an employee, vendor or business partner.
4. Leverage relationships with the audit committee and board to (a) heighten awareness and knowledge of cyberthreats; and (b) ensure the board remains highly engaged with cybersecurity matters and up to date on the changing nature of cybersecurity risk.
5. Ensure cybersecurity risk is integrated formally into the audit plan.
6. Develop, and keep current, an understanding of how emerging technologies and trends are affecting the company and its cybersecurity risk profile.
7. Evaluate the organization’s cybersecurity program, aligning it against an appropriate framework such as the NIST Cybersecurity Framework, ISO 27001/27002 or HITRUST CSF.
8. Seek out opportunities to communicate to management that with regard to cybersecurity, the strongest preventive capability requires a combination of human and technology security – a complementary blend of education, awareness, vigilance and technology tools.
9. Emphasize that cybersecurity monitoring and cyber-incident response should be a top management priority – a clear escalation protocol can help make the case for (and sustain) this priority.
10. Address any IT/audit staffing and resource shortages as well as a lack of supporting technology tools, either of which can impede efforts to manage cybersecurity risk effectively.



ELECTRONIC HEALTH RECORDS, INFORMATION TECHNOLOGY TRANSFORMATION AND DIGITIZATION

Recent technologies – such as connected medical devices, cloud networks and personal health devices – continue to transform the delivery of medical care. Over the past decade, healthcare stakeholders have implemented a health information technology infrastructure to access, send and receive electronic health data.

However, unlike other industries, such as financial services, which have already been transformed by technology, many healthcare organizations have yet to invest sufficiently in robust IT security measures that can protect and encrypt data in electronic health record (EHR) systems, interfaces, repositories, and connected medical and personal devices.

- Overall, technology capabilities dominate the top areas in need of improvement. Respondents gave themselves relatively low competency marks in cloud computing, information security, the NIST Cybersecurity Framework, digital transformation and business intelligence, among other areas.
- The Internet of Things, which is hovering just under the top areas in need of improvement, promises to become an area of increasing focus as wearable, subcutaneous and ingestible monitors and diagnostic technology move from the cutting edge into the mainstream.
- Healthcare industry-specific areas for improvement noted by respondents include DSRIP programs, Medicare cost reporting, health insurance and information exchanges, population health, and state-specific privacy and security laws.
- Of particular concern from an internal audit perspective, the use of health information exchanges is increasing and the risks of moving all patient records to a centralized repository controlled by and connected to multiple third parties are very high.

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

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level
1 (tie)	Delivery System Reform Incentive Payment (DSRIP) program	1.8
	Medicare cost reporting	2.2
3 (tie)	Health insurance exchanges	2.2
	Health information exchanges	2.4
	Population health	2.2
	State-specific privacy/security laws	2.6
7	Cash acceleration programs	2.1
8 (tie)	Information security	3.3
	Risk pool/capitation accounting	2.0
10 (tie)	Pandemic planning/business continuity	2.2
	Intellectual property (research-related)	2.2

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

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level
1	Electronic health records	3.4
2 (tie)	Denials management	3.1
	Physician operations, arrangements and compensation methodologies	3.1
4	Delivery System Reform Incentive Payment (DSRIP) program	1.9
5 (tie)	Information security	3.4
	Patient Protection and Affordable Care Act (ACA) provisions	2.9
7 (tie)	Population health	2.7
	Business continuity and disaster recovery	3.3
9	Hospital value-based purchasing	2.9
10 (tie)	Vendor risk management	3.0
	Clinical documentation	2.5

Table 3: General Technical Knowledge – Overall Healthcare Industry Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level
1	Cloud computing accounting standard	2.1
2	ISO 27000 (information security)	2.3
3 (tie)	Cloud computing	2.7
	NIST Cybersecurity Framework	2.4
5	Business/digital transformation	2.4
6 (tie)	ISO 31000 (risk management)	2.1
	Big data/business intelligence	2.7
8 (tie)	Agile risk and compliance	2.4
	Assurance around outsourced service providers	2.9
	Mobile applications	2.6

Table 4: General Technical Knowledge – CAE Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level
1	Cloud computing	2.8
2 (tie)	Cloud computing accounting standard	2.6
	Mobile applications	2.3
	Internet of Things	2.7
5	Assurance around outsourced service providers	3.1
6 (tie)	NIST Cybersecurity Framework	2.9
	Business/digital transformation	2.9
8	ISO 31000 (risk management)	2.5
9 (tie)	Reporting on Controls at a Service Organization – SSAE 16/AU 324 (also known as SOC1 and SOC reports)	3.0
	GTAG 16 – Data Analysis Technologies	2.6
	Big data/business intelligence	3.1

Table 5: Healthcare Industry-Specific Technical Knowledge – Overall Results, Three-Year Comparison

2016	2015	2014
Delivery System Reform Incentive Payment (DSRIP) program	Health information exchanges	Health information exchanges
Medicare cost reporting	Health insurance exchanges	eDiscovery
Health insurance exchanges	Accountable care organizations	Meaningful Use compliance
Health information exchanges	Patient Protection and Affordable Care Act (ACA) provisions	Coding knowledge (ICD-9, ICD-10, HCC, HCPCS, CPT)
Population health	State-specific prompt payment laws	Healthcare joint ventures
State-specific privacy/security laws	Accreditation environment (e.g., The Joint Commission)	Physician compensation methodologies (e.g., wRVU)
Cash acceleration programs	Ancillary services (pharmacy, lab, radiology, etc.)	Risk pool/capitation accounting
Information security	Cash acceleration programs	Cost containment – labor and non-labor
Risk pool/capitation accounting	Fraud investigations	Delivery System Reform Incentive Payment (DSRIP) program
Pandemic planning/business continuity	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
Intellectual property (research-related)	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 6: Healthcare Industry-Specific Technical Knowledge – CAE Results, Three-Year Comparison

2016	2015	2014
Electronic health records	Cost reporting	Health information exchanges
Denials management	Health information exchanges	IRB and clinical trials
Physician operations, arrangements and compensation methodologies	Health insurance exchanges	Meaningful Use compliance
Delivery System Reform Incentive Payment (DSRIP) program	Medicare cost reporting	Physician compensation methodologies (e.g., wRVU)
Information security	Hospital value-based purchasing	Case management
Patient Protection and Affordable Care Act (ACA) provisions	Reimbursement methodologies (Medicare, Medicaid, etc.)	Coding knowledge (ICD-9, ICD-10, HCC, HCPCS, CPT)
Population health	State-specific prompt payment laws	Delivery System Reform Incentive Payment (DSRIP) program
Business continuity and disaster recovery	Accountable care organizations	eDiscovery
Hospital value-based purchasing		Healthcare joint ventures
Vendor risk management		Pandemic planning/business continuity
Clinical documentation		Physician organizations
		Risk pool/capitation accounting

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

2016	2015	2014
Cloud computing accounting standard	NIST Cybersecurity Framework	Recently enacted IIA Standard: Overall Opinions (IIA Standard 2450)
ISO 27000 (information security)	ISO 14000 (environmental management)	Social media applications
Cloud computing	Reporting on Controls at a Service Organization – SSAE 16/AU 324 (replaces SAS 70)	Mobile applications
NIST Cybersecurity Framework	ISO 9000 (quality management and quality assurance)	Recently enacted IIA Standard: Audit Opinions and Conclusions (IIA Standards 2010.A2 and 2410.A1)
Business/digital transformation	GTAG 16 – Data Analysis Technologies	GTAG 16 – Data Analysis Technologies
ISO 31000 (risk management)	The Guide to the Assessment of IT Risk (GAIT)	NIST Cybersecurity Framework
Big data/business intelligence	ISO 27000 (information security)	GTAG 6 – Managing and Auditing IT Vulnerabilities
Agile risk and compliance	Social media applications	GTAG 15 – Information Security Governance
Assurance around outsourced service providers	Mobile applications	Recently enacted IIA Standards – Functional Reporting Interpretation (IIA Standard 1110)
Mobile applications		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

2016	2015	2014
Cloud computing	NIST Cybersecurity Framework	Mobile applications
Cloud computing accounting standard	Mobile applications	NIST Cybersecurity Framework
Mobile applications	The Guide to the Assessment of IT Risk (GAIT)	Social media applications
Internet of Things	Social media applications	Cloud computing
Assurance around outsourced service providers	2013 COSO Internal Control Framework – Evaluation of "Present, Functioning and Operating Together"	ISO 27000 (information security)
NIST Cybersecurity Framework	ISO 14000 (environmental management)	GTAG 6 – Managing and Auditing IT Vulnerabilities
Business/digital transformation	Reporting on Controls at a Service Organization – SSAE 16/AU 324 (replaces SAS 70)	GTAG 15 – Information Security Governance
ISO 31000 (risk management)	2013 COSO Internal Control Framework – Information and Communication	
Reporting on Controls at a Service Organization – SSAE 16/AU 324 (also known as SOC1 and SOC reports)		
GTAG 16 – Data Analysis Technologies		
Big data/business intelligence		

▨ = Three-year trend

TECHNOLOGY-ENABLED AUDITING AND MANAGING FRAUD RISK

Technology-Enabled Auditing

Digital transformation offers the internal audit function both a challenge and an opportunity.

There are challenges in the sense that as the volume, variety and vulnerability of data increase, so does the scope of risks internal audit must monitor. At the same time, there are opportunities in what could be the "final frontier" for internal audit departments to enhance performance and precision. Technology-enabled auditing tools, processes and practices have made it possible for internal auditors to continuously monitor all data and processes and flag anomalies, instead of sampling and making assumptions.

Data analysis and computer-assisted audit tools are opening new horizons for internal auditors, as operational and risk managers increasingly seek their advice on managing strategic risks.

- New auditing technologies, in general, rank as a top area for improvement among internal auditors in the healthcare industry.
- Respondents singled out data analysis tools along with computer-assisted audit tools as top technology needs.
- Enterprisewide risk management (ERM) – the ability to align bottom-up business unit risk management efforts with automated tools, holistic control frameworks and top-down risk strategies – has emerged as a top priority in the industry. Of note, in June 2016, COSO published an exposure draft of an update to its ERM framework, designed to address the increasing speed and complexity of risk management.

The challenge will be to see where healthcare internal audit shops go from here. Audit technology and data analytics have been cited as critical needs in our broader capabilities and needs survey every year since we began tracking these trends 10 years ago. While internal audit functions remain committed to improving how they leverage technology-enabled audit tools, a decade of results suggests progress is lacking. The question becomes: Why have internal audit organizations been unable to solve this puzzle? Unlike 10 years ago, there are seemingly countless data analysis and technology tools available today, and enterprise resource planning (ERP) systems can perform many of these activities with relative ease.

Bottom line, despite whatever organizational or cultural resistance there may be, now is the time to embrace change and to act. Healthcare internal audit functions that are not leveraging these technologies are likely at a tipping point where technology- and data-driven organizations will soon require an internal audit function with data analysis, continuous auditing and continuous monitoring capabilities. The trend over the past decade is clear. A decade from now, it is very likely that healthcare provider organizations will not be able to afford to have an internal audit shop without these capabilities in place.

Managing Fraud Risk

Healthcare expenditures in the United States topped $3 trillion in 2015, making the healthcare industry a prime target for fraudsters, according to the Centers for Medicaid & Medicare Services.[2] With so much at stake, it's no wonder that fraud monitoring and fraud auditing were cited by respondents to our survey as two of the top ten areas for improvement.

The Department of Justice has made the prosecution of fraud a top priority, with its focus shifting from financial recovery to holding individuals, and corporations, responsible. This includes not only the perpetrator, but also the corporate target, and its officers, if it can be shown that the company didn't do enough to consistently and persistently root out fraud and prevent it from occurring through proper controls and a culture of integrity and accountability.

As a further fraud monitoring activity, internal audit functions should collaborate with their respective compliance departments to assist with the execution of the auditing and monitoring element of effective compliance programs. Internal auditors often have the requisite skills to assist with a number of auditing and monitoring activities listed within the organization's Office of Inspector General (OIG) work plans or annual compliance work plans established to detect and remediate instances of fraud, waste and abuse.

Table 9: Audit Process Knowledge – Overall Healthcare Industry Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level
1	Auditing IT – new technologies	2.9
2	Data analysis tools – statistical analysis	3.2
3	Computer-assisted audit tools (CAATs)	3.2
4 (tie)	Fraud – monitoring	3.3
	Enterprisewide risk management	3.2
6 (tie)	Auditing IT – program development	3.0
	Auditing IT – security	3.2
8	Marketing internal audit internally	3.3
9	Continuous monitoring	3.3
10	Fraud – auditing	3.4

Table 10: Audit Process Knowledge – CAE Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level
1	Auditing IT – new technologies	3.0
2 (tie)	Computer-assisted audit tools (CAATs)	3.4
	Data analysis tools – statistical analysis	3.2
4	Data analysis tools – data manipulation	3.4
5 (tie)	Continuous monitoring	3.4
	Fraud – monitoring	3.8
7 (tie)	Auditing IT – change control	3.3
	Auditing IT – computer operations	3.2
	Auditing IT – program development	3.2
10 (tie)	Continuous auditing	3.4
	Data analysis tools – sampling	3.3
	Marketing internal audit internally	3.5

[2] Centers for Medicaid & Medicare Services, www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsProjected.html.

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

2016	2015	2014
Auditing IT – new technologies	Fraud – fraud risk assessment	Quality Assurance and Improvement Program (IIA Standard 1300) – Periodic Reviews (IIA Standard 1311)
Data analysis tools – statistical analysis	Fraud – fraud risk	Statistically based sampling
CAATs	Fraud – monitoring	Auditing IT – new technologies
Fraud – monitoring	Auditing IT – security	Marketing internal audit internally
Enterprisewide risk management	Continuous auditing	Auditing IT – program development
Auditing IT – program development	Fraud – auditing	Auditing IT – security
Auditing IT – security	Assessing risk – emerging issues	CAATs
Marketing internal audit internally		Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)
Continuous monitoring		Assessing risk – emerging issues
Fraud – auditing		

▨ = Three-year trend

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

2016	2015	2014
Auditing IT – new technologies	Auditing IT – security	Auditing IT – new technologies
CAATs	CAATs	Auditing IT – security
Data analysis tools – statistical analysis	Data analysis tools – data manipulation	Marketing internal audit internally
Data analysis tools – data manipulation	Continuous auditing	Assessing risk – emerging issues
Continuous monitoring	Data analysis tools – statistical analysis	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)
Fraud – monitoring	Marketing internal audit internally	Quality Assurance and Improvement Program (IIA Standard 1300) – Periodic Reviews (IIA Standard 1311)
Auditing IT – change control	Fraud – monitoring	Statistically based sampling
Auditing IT – computer operations	Continuous monitoring	
Auditing IT – program development		
Continuous auditing		
Data analysis tools – sampling		
Marketing internal audit internally		

▨ = Three-year trend

COLLABORATION AND COMMUNICATION BETWEEN INTERNAL AUDIT AND THE ORGANIZATION

The internal audit technical skills we have discussed in our report are critical for healthcare internal auditors. Yet auditing at the speed, precision and complexity necessary for healthcare provider organizations requires more than high-tech tools, a gift for statistical analysis, and knowledge of the numerous laws and regulations under which healthcare providers operate. At the end of the day, the efficacy of an internal audit function also is determined by the ability to partner effectively with others.

In order to perform their jobs at a high level, internal auditors need to serve as strong business partners to others in the organization and, in particular, to be effective persuaders and negotiators. Sometimes the audience will not like the message that internal audit needs to deliver. In these instances, effective skills in negotiating, persuading and presenting come into play. Other important "soft" skills identified as priorities in the survey include dealing with confrontation and high-pressure meetings, and developing outside contacts and networking. Such skills can help establish the internal audit function as a valued strategic partner and trusted adviser.

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

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level
1 (tie)	Persuasion	3.3
	Negotiation	3.2
3	High-pressure meetings	3.3
4 (tie)	Developing outside contacts/networking	3.2
	Developing rapport with senior executives	3.4
	Developing other board committee relationships	3.2
7 (tie)	Time management	3.4
	Developing audit committee relationships	3.5
9 (tie)	Presenting (public speaking)	3.5
	Strategic thinking	3.7
	Leadership (within your organization)	3.4

Table 14: Personal Skills and Capabilities – CAE Results

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Level
1	Presenting (public speaking)	3.8
2 (tie)	Developing outside contacts/networking	3.3
	Negotiation	3.5
	Using/mastering new technology and applications	3.6
5	Developing other board committee relationships	3.9
6 (tie)	Dealing with confrontation	3.6
	Persuasion	3.8
	Time management	3.8
9 (tie)	Change management	3.6
	Developing rapport with senior executives	4.0
	Leadership (within your organization)	3.9

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

2016	2015	2014
▨ Persuasion	High-pressure meetings	▨ Presenting (public speaking)
▨ Negotiation	▨ Persuasion	▨ Developing other board committee relationships
High-pressure meetings	▨ Negotiation	▨ Developing outside contacts/networking
▨ Developing outside contacts/networking	Presenting (small groups)	Leadership (within your organization)
Developing rapport with senior executives	▨ Developing other board committee relationships	▨ Persuasion
▨ Developing other board committee relationships	▨ Developing outside contacts/networking	Time management
Time management	Developing rapport with senior executives	Using/mastering new technology and applications
Developing audit committee relationships	Leadership (within the internal audit profession)	Dealing with confrontation
▨ Presenting (public speaking)	▨ Presenting (public speaking)	Developing audit committee relationships
Strategic thinking	Strategic thinking	▨ Negotiation
Leadership (within your organization)	Using/mastering new technology and applications	

▨ = Three-year trend

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

2016	2015	2014
Presenting (public speaking)	Persuasion	Using/mastering new technology and applications
Developing outside contacts/networking	Strategic thinking	Developing audit committee relationships
Negotiation	Presenting (small groups)	Developing other board committee relationships
Using/mastering new technology and applications	Developing outside contacts/networking	Developing outside contacts/networking
Developing other board committee relationships	High-pressure meetings	Negotiation
Dealing with confrontation	Using/mastering new technology and applications	Presenting (public speaking)
Persuasion	Negotiation	High-pressure meetings
Time management	Creating a learning internal audit function	Persuasion
Change management	Presenting (public speaking)	
Developing rapport with senior executives		
Leadership (within your organization)		

▨ = Three-year trend

CLOSING THOUGHTS

As patient care enters an era of continuous monitoring and hyper-customization, enabled by networked medical devices, big data, and mobile, wearable, subcutaneous and even ingestible technology, major healthcare provider organizations are simultaneously digitizing their business operations and consolidating data throughout the enterprise. This technology wave has sweeping implications for internal audit, demanding continuous auditing, a strong enterprise risk management framework and advanced analytics.

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.

Contacts

Todd Havens
AHIA White Paper Committee Chair
+1.615.875.7728
todd.havens@vanderbilt.edu

Mark Ruppert
Publications Committee Chair
+1.323.866.6900
ruppertm@cshs.org

David Stumph
Executive Director
+1.888.275.2442, ext. 6111
dstumph@kellencompany.com

Dennis Smyser
Board Liaison
dennis.smyser@brooksrehab.org

Michelle Cunningham
Account Executive
+1.888.275.2442, ext. 6120
mcunningham@kellencompany.com

Linda McKee
+1.757.455.7777
lsmckee@sentara.com

Michael Fabrizius
+1.704.512.5900
michael.fabrizius@carolinashealthcare.org

Mark Eddy
mark.eddy@hcahealthcare.com

Debi Weatherford
+1.770.801.2566
debi.weatherford@piedmont.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.

Ranked 57 on the 2016 *Fortune* 100 Best Companies to Work For® list, 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.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

www.protiviti.com