The Institute of
Internal Auditors

Contents

Introduction	1
Talent Management	1
Data Analytics	4
Cyber	7
Regulations	9
Cryptocurrencies	9
Global Data Protection Regulations	10
Responding to Disruption	15
Closing Thoughts	17

Previous Issues

To access previous issues of Global Perspectives and Insights, visit www.theiia.org/GPI.

Reader Feedback

Send questions or comments to globalperspectives@theiia.org.

Introduction

Presenting 2018 — a new year, new laws, regulations, opinions, ideas, technology, and risks. Today's business environment is significantly different than it was in the past; it is more complex and more connected. Organizations face new and unknown risks, but also new and untapped opportunities. Considering in the year ahead the new opportunities and number of potential challenges and risks — some of which are expected and some of which are unique to 2018 — audit plans should be viewed as frameworks that will change as events occur, including those that are disruptive.

With its organizationwide view, internal audit helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve on the effectiveness of risk management, control, and governance processes. Regulators and audit committees want and need assurance that risk management efforts are adequate to address threats posed by formidable competitors, growing technologies, changing marketplace trends, and regulatory developments (see Internal Audit Future Trends: Emerging Trends and High-impact Areas of Focus).

As the need exists for internal audit to provide more value-adding and strategic support to all industries, auditors need to ensure that their work is aligned with all significant risks, especially strategic and operational risks. Internal audit must be responsive and adaptable to a dynamic risk environment.

Risks change, and even the most well-prepared audit plans should be flexible and subject to change as new risks emerge at every level of the organization. This paper discusses the top five risks (to internal audit or the organization) faced by chief audit executives (CAEs), as identified by IIA affiliates. These risks are: Talent Management, Data Analytics, Cyber, Regulations, and Responding to Disruption.

Talent management

Talent management is consistently a top concern of CAEs and internal audit professionals. For the last few years, CAEs have agonized over finding candidates with the skills necessary to fill new roles and address new and existing risks. Plainly, there is a limited pool of candidates with the skills to fill internal audit's evolving needs. In addition, there is the challenge of aligning the work environment with the unique attributes of the millennial workforce, which has greater and different expectations of support and appreciation, a specific work environment in mind, and a preference for more flexible work schedules (see 4 Strategies for Bridging the Internal Audit Talent Gap).

In 2015, *attracting and retaining talent* was a high or critical priority for more than 40 percent of those responding to a global IIA survey, with more than half of the respondents attributing *knowledge gap* to the limited pool of skilled auditors. Again in 2017, in response to an IIA Audit Executive Center® (AEC®) survey, a clear majority (79 percent) of nearly 200 CAEs identified talent management as the top extremely/very important risk to the internal audit profession. According to KPMG, talent — or the lack thereof — is considered by boards as an *enterprise risk*. As organizations become more global, the workforce supporting them continues to evolve, which is why talent management is so critical. The potential impact and implications of the global talent shortage includes the inability to maintain leadership skills, as there is no longer a healthy pipeline of future leaders, and business strategy deliverables are in doubt because candidates are not capable of taking on critical roles.

Organizations are finding that they are not capable of coaching and mentoring new generations or retaining top or specialized talent, causing intellectual capital and competitive advantage to be lost. Further, and constantly, the retiring population triggers skill scarcity (see Boardroom Questions: Talent Management…or Talent Risk?).

To add insult to injury, because of emerging risks — such as data analytics, third-party management, cybersecurity, sustainability, and political and other uncertainties — organizations expect more from their internal auditors. Gone are the days when internal audit's focus is limited to the traditional financial and compliance-based tasks and interests.

While internal audit is not in the business of human resources, internal audit should assess *how well* management is addressing these risks. Today's organizations are in need of, and expect internal auditors to take on, a more holistic approach to auditing, including integrated risk oversight and value creation. Because of this, the search for internal audit top talent, skill, and strength has become very competitive.

Without adequate skills, internal audit is vulnerable to overlooking, or not thoroughly auditing, specific and nontraditional risks, such as technology, geopolitics, economics, evolving corporate reporting, culture, and domestic and global regulations. According to the Society for Human Resource Management, internal audit's ability to evolve beyond traditional financial, operational, and general IT skill sets, and focus on a bigger picture, is crucial.

An internal audit activity that thoughtfully expands its competencies and undertakes its work based on a more comprehensive understanding of the organization's risk profile will be better prepared to serve the organization. Part of that preparation is bringing in people with advanced critical-thinking capabilities and keen business acumen, paired with expertise in specific areas or with industry-specific knowledge. The nontraditional, emerging risks will influence the audit universe; therefore, internal audit must reach for and expand the breadth and depth of its skills.

It is imperative that CAEs lead auditors toward broadening their experience and skills, and consider the "new normal" of risks when assessing and executing audit plans. Make no mistake, traditional audit training is relevant, and will always be relevant; but continuous education and exposure, adaptability, good soft skills, and process and operations knowledge are essential to navigating the new business world.

"If internal audit is to be poised for the future, one of the five imperatives it must address is agility. We must be agile enough to recognize and address emerging risks and to assess risks continuously, then adapt our audit coverage accordingly. And, we must be agile enough to recognize gaps in our capabilities and close them quickly. Success in the future will come to those internal audit departments that have a dynamic talent-management strategy."

Richard Chambers, IIA President and CEO

The ability to manage all talent is vital to internal audit's success, and can bring long-lasting benefits — beyond filling episodic staffing shortages. To optimize talent management efforts, CAEs and senior management should develop well-thought-out and well-developed approaches geared to restructure and enhance their workforce. For effectiveness, and to build, engage, and retain the best internal audit activity possible in the face of new risks, CAEs must develop strategies that include measuring what is needed from their existing staff members, what is needed from the anticipated additions to their staff, and, just as important, what staff members need to see and hear from their leaders to grow and succeed.

A sound talent-management strategy depends on a combination of approaches. CAEs will not be able to hire their way out of a talent shortage. There is a short supply of candidates with skills needed to address tomorrow's risks — including those with skills in data science, innovative thinking, analytical/critical thinking, communication, and others. An effective strategy includes understanding what skills and attributes are needed, and continuous efforts to acquire, develop, and retain top talent.

Objectives

- Internal audit's collective competencies are driven by the risks that drive internal audit's scope. Change listening tours.
- CAEs, the audit committee, and executive management have a strong understanding of the skills needed to support organizational objectives, and the total cost of the internal audit staff.
- Internal audit has implemented a consistent performance management process.
- Internal audit leaders have the capability to coach, mentor, and engage new generations or those of any generation that are new to the profession of internal auditing.
- Formal career plans are in place for all internal audit staff.
- Internal audit has established programs to onboard new employees and continually educate everyone on organizational culture, risk appetite, and strategic direction.

Audit Focus

IIA Standard 1210: Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the know-ledge, skills, and other competencies needed to perform its responsibilities.

IIA Standard 1230: Continuing Professional Development

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

Actions

- Review the risk assessment and audit plan, and identify skills needed to execute the plan. Undertake a gap analysis between the current skills and skills needed and develop a strategy to fill the gaps.
- Structure or restructure performance reviews to include specific job competencies, actionable goals that are in line with the organization's strategic plan, and salary structures for specialty professionals such as data analysts.
- Mentor and develop the skills within the existing staff, which affords the least disruption and integrates existing corporate knowledge with newly required skills.
- Persistently acquire new skills in the marketplace. Look for candidates with different backgrounds, not just those with finance and accounting degrees. Consider third-party service providers as a resource for quickly obtaining skills needed to address complex and specialized risks.
- Establish an effective onboarding and knowledge transfer program.

Audit Focus

IIA Standard 1220: Due Professional Care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

1220.A2 – In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

Data analytics

Data analytics is the process of gathering and analyzing data, and then using the results to make better decisions (*Internal Auditing, 4th edition*, 11-2, Internal Audit Foundation, 2017). Organizations are producing growing stores of data from their operations, which presents two key challenges for internal audit. The first is how to help the board and management understand how that data is being collected, managed, protected, and harnessed. The second is how to exploit the growing data from an internal audit perspective in applying analytics tools to existing audit processes, and automating routine audits and focusing on emerging risk areas (see Risk in Focus: Hot Topics for Internal Audit 2018).

Basically, data analytics breaks down volumes of data, and rebuilds it again in the form of smaller nuggets, providing the opportunity to extract meanings and understandings from the data. With that information, internal audit can analyze *total population* risks and potential correlations, provide insight and foresight, and report on issues that stakeholders are concerned with and are interested in following. Managing data analytics, and the risks associated with it, can be daunting. Deriving meaningful insights from that data — and converting knowledge into action — is, at times, easier said than done. For data analytics to be effective, the right people, formats, processes, and technology need to be in place.

With more data than ever at their immediate disposal, management and the board must realize that massive amounts of data expose the organization to data-related financial and nonfinancial risks. Several risk areas must be addressed in any analytics initiative (see Understanding and Managing the Risks of Analytics):

- **Data and Information Quality Risk** — Decision-makers need data that communicates and promotes an understanding of the complex. There must be clear definitions and quality standards for all data and information.
- **Data and Information Compliance Risk** — Failure to comply with the requirements of an authorized and recognized agent (usually associated with state, federal, or international) can lead to an adverse result such as financial penalty, additional work, or personal liability.
- **Data and Information Governance Risk** — Data and information must be carefully controlled through the use of risk-management principles and processes at the appropriate levels to ensure privacy, security, quality, and auditability.
- **Inappropriate or Premature Use of Analytics Risk** — Analytics will not be helpful when there is no time for gathering, processing, and interpreting data; when there is no history or precedent related to the decisions or when historical data is misleading; or when key variables cannot be measured or have high degrees of uncertainty.
- **Countercultural Impact Risk** — Imposing analytics initiatives in an organizational culture that is not data-oriented can pose a significant risk to leaders; analytics initiatives should include an assessment of the organizational decision-making system and degree to which organizational culture is data-oriented.
- **Data Ethics Risks** — Data analytics initiatives should align with the organization's core values, decision-making, and behaviors. Controls should be in place to ensure the ethical collection and usage of data.

Internal audit should always be aware of the dangers that organizations may face with big data projects, particularly in a situation where the staff lacks some skill. Data analytics demand is on the rise, and soon — if it is not already — it will be an integral part of *every* organization. While it is important for organizations to participate in big data projects to remain competitive and not be left behind, there are risks that need to be considered:

- Data security.
- Data privacy.
- Costs.
- Unreliable, invalid, insufficient, or irrelevant data.
- Unreliable, invalid, insufficient, or irrelevant analytic processes.

Technology changes the world we live in at a lightning pace, and the consequences of that speed of change is frustrating, to say the least, if we are not properly prepared. Technology generates much larger amounts of data, and internal audit can use it to evaluate risks more thoroughly, improve the delivery of audits, and potentially increase the level of assurance provided.

Results from recently conducted case studies show that the key benefits of data analytics for internal audit include increased efficiency, increased effectiveness, improved assurance, greater focus on strategic risks, greater audit coverage, and significant savings in terms of time and money over the long term. However, to experience these benefits, **internal audit must assess how well the data analytics program serves its overarching goals and desired activities.**

Data analytics is vital to internal audit's toolset, as it can provide insights buried deep in the data as well as enable more efficient and effective testing. Many internal audit teams have not yet adopted the more sophisticated data analytics technologies; they are still relying primarily on spreadsheet-based tools and applications. The audit committee's support is essential. Internal audit should make sure the audit committee is educated about the importance of data analytics (see Data Analytics: Is it Time to Take the First Step?).

To build or improve a data analytics program, CAEs should engage in discussion with stakeholders on the desired outcomes, defining analytics objectives and determining what *competencies* and technologies will be required.

One of the main barriers to building an efficient data analytics program — and a constant risk for internal audit — is inadequate skilled staff to handle big data. Because of a deficit in this specialization, internal audit's analytics programs may be less than optimal — not necessarily because of the program itself, but rather because it is not being used to its fullest potential. As with any new business initiative, big data projects involve an element of risk. If the talent to manage big data is missing, it increases the element of risk all the more.

Objectives

- Internal audit has a deep understanding of data analytics and technology, and how advanced technologies can enhance internal audit effectiveness and efficiency.
- Internal audit evaluates how well management responds to new risks introduced from expanded use of data analytics.
- Internal audit makes use of the advanced abilities of data analytics programs for the complete benefit of the organization (e.g., validation of and monitoring for high-risk schemes and behaviors, evaluation and accuracy of risk assessment processes specific to the organization, etc.).
- Internal audit leverages technology for the identification of anomalies and patterns of fraud risk early, and communicates key findings.
- Internal audit leverages technology to enhance the organization's overall risk coverage at lower labor hours and labor costs.

Partially adapted from: First Steps in Building a Data Analytics Program for Your Internal Audit Team

Actions

- Determine what outcomes from the analyses best serve internal audit's objectives, by deciding what the basic and the specific needs are for the data analytics program.
- Understand the benefits that analytics programs could provide to the organization and internal audit in terms of innovation and opportunity. Identify skills required to optimally implement the programs and realize the benefits.
- Consider data analytics as a critical business component, and customize the audit engagement to receive the best possible sustainable, quality approach to managing the organization's entire compliance and controls framework.
- Engage with management on specific rules, data points, codes, and assumptions in the program that will accurately detect irregularities or patterns of fraud.

Cyber

Whether it is the relentless onslaught of information breaches against organizations or the never-ending accounts of personal identity theft, cybercriminals — sophisticated and well-funded — are formidable opponents. Interconnectedness makes for a complex and risk-based world, just ripe for cybercriminals. The techniques that they use continue to expand and evolve; so much so, that it is a chore to keep up with them.

Launching a defense plan against cyberattacks, and ensuring that the plan is effective, is a 24-hour job; it is not a matter of *if* an attack will occur but *when*. There is a big difference between cyber risk awareness and cyber risk *preparedness*. All are *aware* of the risks; we are faced with the truth of it daily. Preparedness, however, includes the ability to *thwart* an attempted attack entirely, or *withstand* an attack and recover with relatively little or no damage. For organizations to enjoy even a shred of protection against the calamity of a breach, they need to be able to resist, react to, and recover from cyberattacks — *cyber resilient*.

As the concern for cyber issues (e.g., hacking/intrusions, spear fishing, economic espionage, etc.) increases, stakeholders are requiring greater visibility into their organizations' cybersecurity risk management programs, and boards want internal audit's independent, objective, and comprehensive review of cyber risks and cyber programs. Therefore, internal audit also must be knowledgeable of possible risks, and play an important role in cyber resilience.

Unfortunately, cybersecurity risk is not limited to external threats; potential threats can result from the actions of employees or business partners. Therefore, a crucial component of cyber resilience is the proper and effective management of an organization's culture, as well as the evaluation of its *risk*. When considering culture, boards also are including *risk culture*, because it is the basis of all decisions, conduct, and risk taking within the entire organization. Internal audit can audit risk culture within standard operational and financial audits by gathering data and conducting informal reviews.

Leading the charge, internal audit can strengthen management's understanding of the effectiveness of cybersecurity controls in all areas, even at the level in which an organization's culture impacts requirements, processes, and capabilities. Culture drives productivity, values, attitudes, and practices within an organization, and is shaped and maintained by many different factors; therefore, internal audit can assess culture for risk in the same way that it assesses other areas of an organization (see Internal Audit Future Trends). Internal audit can maximize its value by understanding how to evaluate culture, and educating management on its importance.

In order to overcome cyber-related risks, including culture, it is critical that the leadership team develop precautionary measures, put them in place with training and awareness programs, and then ensure that they are continuously demonstrated in behavior. Therefore, employees, vendors, partners, and contractors alike must be trained and made to understand exactly what is expected of them with regard to cybersecurity measures and protocols.

Internal audit's risk assessment strategies should be developed with regard to all risks specific to cybersecurity, and ensure compliance with policies and internal controls. Internal audit needs to develop an intense audit approach that meets the needs of the organization and its stakeholders in all areas where cyber issues can reach. For effectiveness, this requires the installation of — at a minimum — control activities, a control environment, risk assessment, communication, and monitoring, as well as a framework for assessing the cybersecurity measures (see Risk in Focus: Hot Topics for Internal Audit 2018).

As the third line of defense, internal audit should work with management and the board as they develop the cybersecurity strategies and policies to improve the organization's ability to identify and mitigate cybersecurity risks; leverage relationships with the audit committee and the board, making sure that they stay engaged; and make sure that cybersecurity risk is formally integrated in the audit plan, with the necessary skills (in house or through cosourcing) to execute the plan. Emerging technologies and trends affect an organization's cybersecurity risk profile; because of this, internal audit should also stay abreast of emerging technologies and evaluate the organization's level of vulnerability, and its risk activities against the preferred cybersecurity plan.

"Directors don't need to be technologists to play an effective role in cyber risk oversight — but every board can take the opportunity to improve the effectiveness of their cyber-oversight practices."

NACD Director's Handbook on Cyber-Risk Oversight, National Association of Corporate Directors (NACD), 2017

Source: The Value of Visibility: Cybersecurity risk management examination

Objectives

- The organization has a cyber resilient culture.
- Internal audit contributes *key components* crucial to cybersecurity examination and preparedness:
  - Protection and Detection: Internal audit provides a holistic approach to identifying where an organization may be vulnerable, and incorporates data analytics in its realm of responsibility, which will give an alert that something is wrong.
  - Business Continuity: Internal audit provides advice, engaging with management as they plan to deal with and overcome risk scenarios that could impact ongoing operations, including cyberattacks, natural disasters, or succession.
  - Crisis Management/Communications: Internal audit helps with crisis management planning and communications preparedness by providing assurance checks for effectiveness and timeliness, and conducting analyses and critiques of executed plans.
  - Continuous Improvement: Internal audit adds value by providing insight, and improving strategies and protocols for better cyberattack preparation.

Actions

- Assess organizational culture with regard to cyber resilience.
- Perform risk assessments of security models and cybersecurity processes and make recommendations for improvement.
- Perform data penetration testing with IT and third-party contractors to assess the third party's ability to comply with the established protocols.
- Conduct cyber resilience gap analyses, recommend remediation, and follow up on remediation activities.
- Influence culture by emphasizing cybersecurity monitoring and response as top priorities.
- Ensure that the business continuity plan is periodically tested and corrective action is taken for any deficiencies identified.
- Implement and encourage a strong cyber culture and risk culture throughout the organization, which, over time, will influence and increase cybersecurity measures and protocols.

Regulations

Globally, organizations face new or modified regulatory requirements, designed in part to protect consumers or the public interest. The most high-profile regulations focus on financial risks and controls, and data privacy and security, and they impact organizations across all industries.

Cryptocurrencies

According to CNBC, cryptocurrencies could pass the trillion-dollar mark in terms of value, following a recent intense sell-off across digital coins. Bitcoin value is volatile: In early 2018, it fluctuated between $6,000 and $10,000. Thomas Glucksmann, head of APAC business development at cryptocurrency exchange Gatecoin, stated, "Increasing regulatory recognition of cryptocurrency exchanges, the entrance of institutional capital, and major technology developments will contribute to the market's rebound and push cryptocurrency prices to all new highs this year. There is no reason why we couldn't see Bitcoin pushing $50,000 by December (2018)."

Globally, as major financial institutions get more involved in blockchain technology and cryptocurrency trading, they need to figure out how to handle conflicts that could arise when employees trade digital coins in their personal accounts. The soaring prices of digital coins have not only piqued the interest of investors and banks, but compliance departments are paying very close attention. Conflicts could arise if employees involved with — or those who want to invest in — cryptocurrency place bets with an unfair advantage. Generally, employees must get a clearance before trading in any securities that represent a conflict of interest; however, policies are much harder to enforce with cryptocurrencies, as trades are done through a fragmented network of exchanges — sometimes anonymously — and are complicated to track.

In addition, there is the absence of clear rules from global regulators, making it harder for financial organizations to set their own. Some consider cryptocurrencies as commodities, and others say that some cryptocurrencies may be securities, but do not specify which ones. Global regulators have been anxious due to the recent explosive volatility in the value of Bitcoin and other digital currencies, and hard-hitting regulations may be put in place (see Compliance Officers Sweat as Cryptocurrency Trades Go Mainstream).

Audit Focus

IIA Standard 2130: Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

1130.A1 – The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

Global data protection regulations

A number of governments are implementing increased regulations over privacy of data. Two examples are the European Union (EU) and China.

After four years of preparation and debate, the EU's General Data Protection Regulation (GDPR), which replaces the Data Protection Directive 95/46/EC, was approved by the EU Parliament in April 2016. The GDPR becomes effective in May 2018, at a time when year after year, data breaches prove bigger, more intrusive, and more costly. Data breaches increased substantially in 2017 over and above the reported data increase of 40 percent from 2015 to 2016. (For additional details, see "2017 Data Breaches," next page.)

> *"GDPR and the implications of that are gaining prominence. From an assurance perspective, the audit committee will want us initially to assess the program itself but then for us to develop our own program on an ongoing basis to make sure the business has the right processes in place in order to continue complying."*
>
> CAE of a multinational banking group
>
> **Source:** Risk in Focus: Hot Topics for Internal Audit 2018

Although many companies have privacy policies consistent with the old directive, the new GDPR contains a number of new protections for EU data, and promises to fine or penalize data controllers and processers for noncompliance once it becomes effective. Simply put, any organization (local or international) that does business in Europe or handles the personal data of EU residents must comply with the new rules.

For the most damaging breaches of non-compliance with key provisions, regulators have the authority to levy a fine in an amount that is up to the greater of €20 million or 4 percent of global annual turnover in the prior year. There is a tiered approach to fines (e.g., a company can be fined 2 percent for not having their records in order [Article 28], not notifying the supervising authority and data subject about a breach, or not conducting an impact assessment). It is important to note that these rules apply to both controllers and processors — meaning cloud servers will not be exempt from GDPR enforcement. Other examples that fall under this category are non-adherence to the core principles of processing personal data, infringement of the rights of data subjects, and the transfer of personal data to third countries or international organizations that do not ensure an adequate level of data protection (see The EU General Data Protection Regulation).

2017 Data Breaches

Month	Organization	Violation/Breach
Jan. 8, 2017	E-Sports Entertainment Association (ESEA)	1,503,707 records added to its database and leaked records included personal/private information.
Feb. 2, 2017	Xbox 360 ISO and PSP ISO	1.2 million Xbox 360 ISO users and 1.3 million PSP ISO affected; personal/private information was stolen.
March 15, 2017	Dun & Bradstreet	Over 33 million corporate contact shared across the web, including the U.S. Department of Defense and the U.S. Postal Service; personal/private information was leaked.
April 6, 2017	FAFSA: IRS Data Retrieval Tool	Up to 100,000 taxpayers/students may have had personal/private information stolen.
May 10, 2017	Bronx Lebanon Hospital Center	At least 7,000 patients between 2014 and 2017 may have had extremely personal information compromised, including addictions, mental and medical health diagnoses, HIV status, and assault reports.
June 20, 2017	Deep Root Analytics	Roughly 198 million American citizens impacted, as Deep Root Analytics, hired by the Republican National Committee, stored private/personal information on a cloud server without password protection, exposed for over two weeks.
July 13, 2017	Verizon	14 million subscribers' information exposed, as records were held on an unsecured server; data obtained were log files, generated when customers contacted Verizon via phone.
Aug. 30, 2017	Online Spambot	711 million email addresses and passwords harvested from an unsecured server.
Sept. 7, 2017	Equifax	143 million customers may have been affected due to hackers exploiting a weak point in website software; personal/private information exposed, including social security numbers and credit card numbers.
Oct. 12, 2017	Hyatt Hotels	Unauthorized access to payment information for debit and credit cards, including credit card numbers, internal verification codes, and cardholder names that were used (swiped) at 41 properties in 11 countries.
Nov. 21, 2017	Uber	Personal information of 57 million drivers and customers exposed, including names, email addresses, and telephone numbers.
Dec. 10, 2017	TIO Networks (PayPal)	Over 1.6 million customer identities compromised, including bank account information, payment card information, passwords, usernames, and social security numbers.

Adapted from: 2017 Data Breaches – The Worst So Far

Even the definition and conditions of "consent" are significantly restricted. Previously, data controllers were allowed to rely on implicit and "opt-out" consent in some circumstances. As of May 25, 2018, the GDPR strengthens conditions for consent, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in clear and plain language. It must be as easy to withdraw consent as it is to give it. Further, once consent is withdrawn, data subjects have the right to have their personal data *erased* and no longer used for processing (see The Top 10 Operational Impacts of the EU's General Data Protection Regulation).

The GDPR will significantly affect Germany's cybersecurity efforts. In May 2017 the legislature adopted a revised version of the Federal Data Protection Act, which will come into effect together with the EU GDPR on May 25, 2018. Known for its strong national data protection laws, with fines up to €300,000, Germany is now moving to strict cybersecurity standards and assigning the responsibility to protect users and secure cyber information to service providers and operators of critical infrastructure. The new act contains 85 provisions, several of which cross-reference to the EU GDPR. The operators of critical infrastructure must implement appropriate organizational and technical safeguards and other measures in accordance with the *state of the art* within two years after the entry into force of secondary legislation specifying those safeguards.

Audit Focus

IIA Standard 2120: Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

Additionally, critical infrastructure operators must regularly prove that they fulfill the security requirements, and notify the *Bundesamt für Sicherheit in der Informationstechnik* (BSI) immediately of any significant disruptions of the availability, integrity, authenticity, and confidentiality of their IT systems, components, and processes, which may result or have resulted in the failure or an impairment of the functioning of critical infrastructure operated by them (see What You Need to Know About Germany's Cybersecurity Law).

While China already had strict laws, rules, and regulations relating to information security, it introduced an extensive law that bridges the gap between cybersecurity and data protection (effective June 2017), which merges the provisions of the EU's GDPR. In many respects, the Cybersecurity Law of the People's Republic of China (CSL) accords with the GDPR (see Risk in Focus: Hot Topics For Internal Audit 2018). The CSL made amendments that pay more attention to the protection of personal information and individual privacy, and standardizes the collection and usage of personal information. For example, previously, foreign enterprises transferred information outside of China; now, the law stipulates that sensitive data must be stored domestically, and there are strong penalties for violating the law, including suspension of business activities. Fines may reach RMB1,000,000. (For additional details, see "Amendments to the CSL," next page.)

Amendments to the CSL

Article	Final Version	Significant Amendment
31	Regarding cybersecurity protection, the state emphasizes the protection of critical information infrastructure in ***public communications and information services, energy, finance, transportation, water conservation, public services and e-governance***, as well as other critical information infrastructure that could cause serious damage to national security, the national economy and public interest if destroyed, functionality is lost, or data is leaked.	This article clarifies the industries and sectors in which the protection of critical information infrastructure will be given priority.
43	Individuals have the right to require network operators to correct errors in personal information collected or stored by them. ***Network operators should take measures to remove or correct the errors.***	This article gives citizens greater rights to protect their personal information, and increases the network operators' obligation to correct errors in a timely manner.
46	Individuals or organizations ***are responsible for the use of their networks***, and shall not set up websites or communications groups for fraudulent purposes or other illegal activities.	This article emphasizes that individuals and organizations bear the responsibility for the use of their networks.
76(5)	"Personal information" refers to all kinds of information, recorded electronically or through other means, that can determine the identity of natural persons independently or in combination with other information, including, but not limited to, a ***natural person's*** name, date of birth, identification number, personal biometric information, address, and telephone number.	This article expands the scope of personal information protection from "citizens" to "natural persons."
63	People who violate Article 27 of the law and engage in activities that endanger cybersecurity may be detained for 5 to 15 days and may be fined ***RMB100,000–RMB1,000,000***, depending on the severity of the case.	The maximum penalty for violating the Cybersecurity Law has been increased to RMB1,000,000.

Source: Overview of China's Cybersecurity Law

But CSL is not without opposition. As reported by The New York Times in May 2017, "a coalition of business lobby groups representing European, American, and Asian companies called on China to delay implementing the law, while the European Union Chamber of Commerce in China asked for additional time to allow companies to adhere because of the 'substantial compliance obligations.'"

Whether doing business in the EU, China, or any of a number of other countries with increasing regulations regarding data privacy, organizations are feeling the effects. Boards are pushing for enhanced governance frameworks within their organizations, and the boards are being pushed by regulators, investors, and other stakeholders who are holding them accountable for the effectiveness of their overall processes (see Of Corporate Governance, Risk Management, and Internal Audit). The new regulations increase costs and place pressure on organizations by adding complexity to risk management, control, and governance processes.

As the pressure on boards increase, pressure also is placed on internal audit. Organizations are looking to internal audit with great expectation. They recognize the need for internal audit to provide advice and assurance as they redirect disruptive forces into oppor-tunities, while at the same time staying in compliance with the constant change in regulations (see KPMG Internal Audit: Top 10 Key Risks in 2016).

The key to surviving disruptive forces is the achievement of govern-ance, risk management, regulatory compliance, and a balance of performance. Meeting these challenges can protect and enhance business value and drive operational efficiencies.

Objectives

- Clarification of risk appetite when evaluating projects and strategies.
- Organizationwide awareness of current national and international regulations.
- Establishment of measures for compliance with current national and international regulations.
- Coordination of internal and external assurance providers.

Actions

- Understand international compliance frameworks and assurance standards.
- Perform an inventory over existing regulatory bodies and their requirements.
- Assess the organization's approach to managing its global compliance activities, including integration of newly acquired organizations.
- Evaluate the organization's response to notable instances of non-compliance.
- Review compliance training programs, and evaluate the appro-priateness for respective roles.
- Coordinate with internal and external assurance providers to ensure proper coverage and minimize duplication of efforts.
- Craft communications tailored to the organization's interests and priorities to encourage a culture of compliance.
- Evaluate the organization's assignment of responsibilities for regulation compliance.

Audit Focus

IIA Standard 2210: Engagement Objectives

Objectives must be established for each engagement.

2210.A3 – Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board.

IIA Standard 2050: Coordination and Reliance

The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

Responding to disruption

A new day — a new bell, a new whistle. Today's technology changes constantly; it's faster, stronger, bigger (and smaller); it reaches further, and is more intense. It is as never before. Each day internal auditors are faced with new opportunities to provide insight and foresight to stakeholders, but they may not have developed innovation-related skills such as critical thinking and creativity. Consequently, without innovation, they find themselves unable to handle the unexpected and vulnerable to complacency. Internal auditors must adapt their methodologies to utilize technology — to become agile and proactive, and quickly change direction to keep pace with innovation.

"I passionately believe that internal audit has a vital role to play in the success of our organizations. But I also believe that to be up to the task, we need to refresh our commitment to innovation in internal audit. Innovation must be at the core of internal audit's remit if it is to keep pace with the developments in our own organizations and beyond."

Shannon Urban, IIA North American Board Chairman (2017–2018)

Source: Internal Auditor

While innovations, such as new technologies, offer great opportunities for internal audit to perform audit engagements, in many instances, innovation is accompanied by new risks, threats, and *disruptions*, which add to internal audit's concerns. For example, instead of (traditionally) focusing only on risks, internal auditors now need to be able to quickly *identify* the would-be disruptions and determine which ones warrant immediate or additional attention.

One of the main reasons an organization should innovate is to separate itself from the competition — and internal audit can lead the charge. According to the 2018 North American Pulse of Internal Audit, innovation presents internal audit with two options: either re-envision its capabilities to fill an increasingly important role in an organization, or presume past practices and carry them into the future. The latter is a near guarantee of future failure; therefore, internal audit must be open to creative (or even radical) ideas, and be ready and willing to focus on the effective management of related risks.

There will be challenges. Management may be uncomfortable at the thought of doing things differently; budgets may be constrained by the business environment, and the candidate pool may be shallow when it comes to the required skills. But the good news is that internal audit is not alone. Internal audit can learn from other business units, organizations, or internal audit activities that have already developed specific techniques to manage the innovation process.

Innovation — when embraced in the right way — is extremely valuable to internal audit and the entire organization:

- Costs are reduced.
- Value is increased.
- Growth and improved performance is realized.
- Products and services are launched sooner.
- Customer experience and satisfaction is improved.
- Organizational flexibility and agility is amplified.
- Stakeholder satisfaction is increased.

Not only does innovation lead to better and more efficient auditing, but innovation directly supports agility when it enables a faster, smarter, and more focused response to disruption (see 2018 North American Pulse of Internal Audit: The Internal Audit Transformation Imperative). The IIA's Chairman of the North American Board Shannon Urban encourages innovation in internal auditing as both crucial for its growth and necessary in meeting the everchanging needs of stakeholders. It may be a bit uncomfortable and frustrating, but it is ongoing, and demands commitment and courage. Innovation can also be very rewarding. If internal audit wants to understand its stakeholders, and serve them well into the future, embracing innovation is the only option (see The Innovative Internal Auditor).

Objectives

- Internal audit recognizes changes in the business environment.
- Internal audit aims to develop a culture of innovation, and strengthen capabilities and performance.
- Internal audit aims for best practices and obtainable improvements through innovation.
- Internal audit strives for more efficiency through innovation.

Actions

- Design and implement new ideas, making innovation a core foundation to the practice of internal auditing.
- Assume a leadership role, anticipate business disruptions, monitor changes in the environment, and offer a broader range of responses.
- Build and invest in relationships. Stay connected to the business and be aware of innovation taking place.
- Clarify the evolving risk landscape by determining which disruptions warrant additional attention.
- Provide insight and a point of view around emerging risks associated with disruptive events.
- Find and attract candidates with the right competencies to swiftly and decisively respond to new or emerging risks.
- Collaborate with other risk management and compliance functions. Evaluate the organization's assignment of responsibilities for regulation compliance.

Closing thoughts

The risks highlighted in this report — while identified as the top areas of concern by The IIA's affiliates — do not represent all risks to organizations or internal audit. In addition to these areas, affiliates also identified risks inherent to the audit committee, the budget, lines of defense, and strategy — all essential areas of organizational governance that need to be acknowledged and examined. Risk opens the door for failure to achieve an organization's mission and strategic objectives, and threatens an organization's overall value. Therefore, internal audit's responsibility — as a trusted advisor to assist risk management, control, and governance processes — requires the consideration of all risk opportunities and making the right recommendations.

Worldwide, organizations rely on internal audit, and its assessments. To remain relevant and to be recognized as a trusted advisor, internal audit has an obligation to consider risks to the achievement of its own objectives, as well as the objectives of the organization. Because of this, internal audit must be results-focused and committed to improving its abilities for the benefit of the organization as a whole. This requires the ability to rise above challenges and obstacles, including thinking critically; remaining independent and objective; staying agile; focusing on *leadership* against risk — real or imagined; navigating the "times" by functioning as a consultant when needed; providing assurance when needed; and understanding the inter-dependency of all systems, processes, regulations, and operations.

IIA Affiliates

IIA Affiliates are the building blocks of The IIA. The IIA partners with IIA Affiliates in more than 170 countries and territories to fulfill its mission to advance the internal audit profession and serve its more than 190,000 members globally. IIA Affiliates serve as The IIA's exclusive representatives who collectively carry the voice of the internal audit profession promoting high standards of ethics and professional practice in their internal audit communities.

About The IIA

The IIA is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The IIA's global headquarters are in Lake Mary, Fla. For more information, visit www.theiia.org.

Disclaimer

The opinions expressed in Global Perspectives and Insights are not necessarily those of individual contributors or of the contributors' employers.

Copyright

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101