Auditing Emerging Technologies

Facing New-Age Challenges

With unprecedented advances in information technology, audit professionals need to gear up to face the challenge of auditing emerging technologies. Auditors need to learn and understand new skills and acquire knowledge related to predictive analytics, robotic process automation (RPA), blockchain, machine learning and artificial intelligence (AI). Enterprises are adopting emerging technologies at a rapid pace to create synergies and harness the latest technologies, and they expect auditors to be forward-looking technology consultants who can add value to the organization during IT projects. Boards and C-level management use the audit as the primary tool in assessing strategic risk, provided their auditors possess the necessary competency and capacity. Therefore, audit chiefs are always engaged in updating the technology-related skills of their audit workforce.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) guidance explains that although the use of modern technologies has resulted in large amounts of information being processed by automated procedures, internal control principles such as segregation of duties (SoD), maintenance of records, independent reviews, etc., remain suitable and relevant.[1]

Assessing the Risk of Emerging Technologies

Management expects auditors to provide independent opinions during the technology selection process, during pilot testing and project deployment, and after implementation. The paradigm shift from traditional procurement and governance practices has impacted the risk profiles of various entities, and auditors need to adjust their auditing lenses and rethink their assessment of third-party risk, outsourcing, application controls, data privacy and cybersecurity.

Modern technologies—whether, for example, blockchain, AI, RPA or the Internet of Things (IoT)—combine software modules, databases, connectivity interfaces and peripheral devices. The attribute that makes each technology different is the way it affects the business model. Auditors are expected to understand the risk inherent in the technology under review. COBIT® and COSO frameworks apply equally when assessing emerging technologies. Given the disruptive nature of emerging technologies, the methodology for evaluation can change while the underlying assessment processes remain the same.

Figure 1 demonstrates how auditors can leverage the Emerging Technology Analysis Canvas (ETAC)[2] to identify and assess the risk of emerging technologies.

> "GIVEN THE DISRUPTIVE NATURE OF EMERGING TECHNOLOGIES, THE METHODOLOGY FOR EVALUATION CAN CHANGE WHILE THE UNDERLYING ASSESSMENT PROCESSES REMAIN THE SAME."

To outpace competitors, organizations are competing to embrace emerging technologies for harnessing value to their businesses. This often results in neglecting the risk inherent in evaluating, selecting, implementing and operating business activities. Such practices may result in reputational

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2UlljQw

Muhammad Asif Qureshi, CISA, CIA, CISSP, PMP
Is a governance, risk and compliance (GRC) professional with an extensive information systems auditing background. He is currently GRC manager with Tawazun Economic Council, where he was involved in developing the information security department from the ground up and has been an integral part of the team dedicated to building the organization's information security architecture. Qureshi also participates in mentoring and coaching activities at schools and colleges and has been a guest speaker on cybersecurity-related topics for students.

Figure 1—ETAC and COBIT Mapping			
ETAC		**Mapping**	**Auditor's Assessment**
Condition	**Description**		
Opportunity/trigger	Problem the technology resolves	COBIT: Align, Plan and Organize (APO)02; APO03; APO04; APO12; APO13; Build, Acquire and Implement (BAI)02; BAI03 COSO: Control environment, risk assessment	• What is the business opportunity the emerging technology offers the entity? • What is the strategic, legal, regulatory, compliance, operational and technology risk encountered if the entity takes advantage of this business opportunity? • What is the adequacy of controls and residual risk and risk appetite?
Impact	Changes/disruption due to introduction of the technology	COBIT: APO02, APO03, APO12, BAI05, BAI06, BAI07 COSO: Control environment, risk assessment	• How will the new technology change the business strategy? • What are the applicable laws (e.g., labor laws in case the change results in redundant human resources)? • Will laws and regulations require a change in business practices? • How will the existing control environment be affected by the introduction of the new technology? • Is management aware of the risk inherent in the new technology? • How will the introduction of the new technology impact the entity's risk appetite? • How mature is the technology in terms of internal controls? • How will corporate information be protected?
Feasibility	Technical challenges, required skills, tools and best practices; friction while deploying the technology	COBIT: APO03; APO04; APO05; APO06; APO07; APO09; APO10; APO13; BAI04; BAI06, BAI07, BAI08; Deliver, Service and Support (DSS)04; DSS06 COSO: Control environment, information and communication, control activities, monitoring	• Is the entity prepared to embrace this technology in terms of corporate culture and organizational behavior? • Do auditors possess the required knowledge and skills to review the technology? • Have information security and privacy considerations been taken into account? • Has the emerging technology been tested by management, and were the results satisfactory? • Is there an arrangement for secure and resilient IT resources to support the technology? • Does the entity have sufficient staff to manage and operate this technology? • Depending on the type of business, how will customers be impacted as a result of this technology? • Do suppliers of the technology have adequate resources to support the entity?
Future	Speed with which the technology can be deployed and adopted	COBIT: APO02, APO05, BAI01, BAI10, DSS04, DSS05 COSO: Information and communication, control activities, monitoring	• Is there a technology deployment strategy that is aligned with the business strategy and management expectations? • Is the deployment strategy mapped with best practices used for deployment, such as Cloud Security Alliance (CSA) guidelines for cloud computing?
Note: COBIT® domains can be included or excluded as needed.			

damage, adverse market growth and noncompliance with regulations.

Cloud Computing

Cloud computing has been around for a while and is a relatively mature technology. Lower IT costs, a flexible operating model and enhanced availability are some key benefits of cloud computing. A business system on a cloud computing platform is available around the clock, with negligible downtime. However, clouds pose potential risk related to physical access, data privacy, partitioning or segregating server and network resources with other tenants, and applicable laws and regulations. One real-life example comes from Amazon Web

Services: Technical issues resulted in outages of 36 hours for more than 70 clients (far exceeding Amazon's marketing promise of 4.4 hours annually).[3]

When performing audits of cloud-based systems, auditors should refer to best practices such as "Security Guidance for Critical Areas of Focus in Cloud Computing V4.0."[4] These guidelines are divided into 14 domains and are in line with the US National Institute of Standards and Technology (NIST) model for cloud computing and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards (**figure 2**). The guidelines discuss cloud models and related risk and controls, and they are equally beneficial for cloud service providers, their customers and other relevant stakeholders.

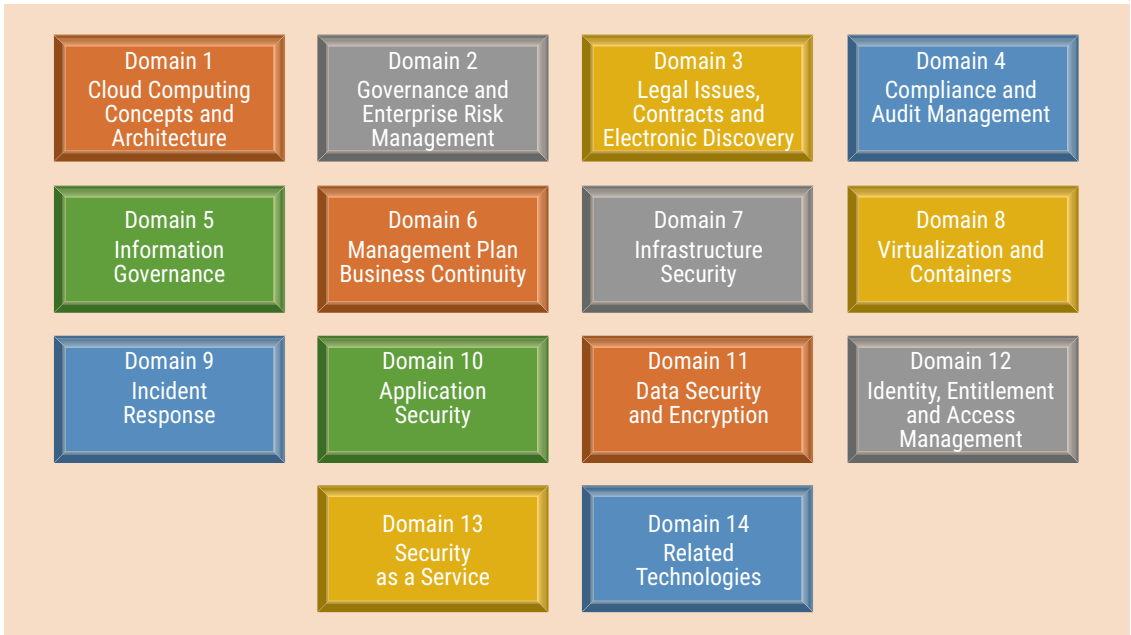
Cloud computing opens up organizations to new risk as cloud computing often involves a third party providing the cloud services. Risk factors such as service level agreements/contracts, information privacy and protection, and compliance with legal and regulatory requirements are a few, along with cloud security controls, access management, information communication and retention, and change management. While assessing the risk associated with cloud computing, auditors need to be aware of cloud service models (i.e., software as a service, platform as a service or infrastructure as a service) being provided to the organization. Additionally, auditors must consider the deployment model (i.e., public, private, hybrid). There is less physical control over assets and greater reliance on external audits for assurance of information protection.

Artificial Intelligence

Artificial intelligence (AI) refers to a system or a machine that can think and learn. AI systems utilize data analysis and intelligent algorithms to make decisions based on predictive methods. Complex algorithms are developed to propose decisions based on a pattern or behavior learned over time. AI has applications in many industries; it is being used in the hospitality industry for room reservation and call center systems, in the aviation industry for ticket booking and predictive maintenance, and in food and beverage operations.

Given the invisible nature of algorithms, audits must focus on the logical flow of processes. A review of AI should ascertain whether unintended bias has been added to the algorithms. Auditors should assess the effectiveness of algorithms and whether their output is appropriately reviewed and approved. Because AI is built on software modules, auditors must also consider cybersecurity and search for possible bugs and vulnerabilities that can be exploited to impact AI functionality. Internal

Figure 2—Security Guidance for Critical Areas of Focus in Cloud Computing



auditors can use the Institute of Internal Auditors (IIA) AI Auditing Framework.[5, 6] This framework is composed of two parts and has three components—AI strategy, governance and human factor—and provides guidance on how to audit AI during different stages of its development and deployment.

Internet of Things

Imagine that a refrigerator could place an order with a grocery store whenever the supply of eggs falls below a certain number. Soon, everything in homes will be connected to the Internet. Components of industrial machines and parts in planes and ships will be able to collect and analyze data and send messages to maintenance organizations, reporting expected breakdowns. Forrester has predicted that cybercriminals will target IoT devices for ransom.[7] This means that attackers will target both customers and their IoT devices for ransom.

Key components of IoT are data collection, analytics, connectivity, and people and process.[8] This is the kind of disruptive technology that auditors should keenly follow because IoT not only changes the business model, but also affects the strategic objectives of the organization. The risk profile of the entity changes with exposure to new laws and regulations.

Due to a heavy reliance on the Internet, auditors must focus on risk related to data privacy, hacking, interruption of services and cybersecurity. Auditors can use NISTIR 8228 (Considerations for Managing Internet of Things [IoT] Cybersecurity and Privacy Risks) for security and privacy of IoT.[9] These guidelines short-list three high-level goals: protect device security, protect data security and protect individual privacy. The guidelines outline relevant risk that needs to be mitigated to meet these three goals.

Blockchain

Blockchain's first implementation was Bitcoin. Since then, blockchain has been adopted by various industries to address several business challenges. Blockchain is based on a decentralized and distributed ledger that is secured through encryption. Each transaction is validated by the blockchain participants, creating a block of information that is replicated and distributed to all participants. All blocks are sequenced so that any modification or deletion of a block disqualifies the information. Despite resistance from the financial industry, the benefits associated with blockchain technology are being recognized across a variety of other industries. Blockchain users include De Beers, Accenture Insurance, MedicalChain, BitProperty, AidCoin, Ripple and Circle.

> "WEAK BLOCKCHAIN APPLICATION DEVELOPMENT PROTOCOLS ARE SOMETHING AUDITORS CANNOT OVERLOOK."

Blockchain is an emerging technology that lacks a uniform auditing standard. ISACA® recently issued an audit program to help identify and develop key policies, procedures and controls to mitigate risk and streamline processes related to blockchain. The audit program is built on six categories: pre-implementation, governance, development, security, transactions and census.[10]

Although blockchain's core security premise rests on cryptography, there are risk factors associated with it. As blockchain interacts with legacy systems and business partners, concerns related to insecure application programming interfaces (APIs), data confidentiality and privacy cannot be ignored. Weak blockchain application development protocols are something auditors cannot overlook. Similarly, data privacy laws and regulations may be problematic as data are communicated across geographic boundaries. Auditors must be able to determine whether the data put on blockchain will expose the enterprise to liability for noncompliance with applicable laws and regulations.

Robotic Process Automation

Process efficiency, customer experience and control effectiveness have always been on management's agenda. As the name suggests, RPA is the automation of the repetitive processes performed by users.

Process automation is not limited to one industry or one process; it spans from the manufacturing industry to the financial industry to the pharmaceutical industry. Robotic car manufacturing has been around for a while and is a classic example of process automation, where the output of one process becomes the input of the next process. However, RPA differs because it does not involve physical robots like those used in car manufacturing.

Not all RPA needs an auditor's attention. It depends on the type of process being automated and the complexity of the automation process itself, along with regulatory compliance and business continuity aspects that can raise the risk level of a robotic process.[11]

In a few years, it will be the norm for auditors to add RPA to their scope of work. Although RPA offers consistency, it is prone to elicit a knee-jerk reaction when the dependent processes or systems are exposed to a cyberattack. It is, therefore, of utmost importance for auditors to understand RPA processes, which include data extraction, aggregation, sanitization and cleansing. Unless auditors understand these processes, they will not be in a position to initiate an audit. Similarly, a comprehensive assurance process might demand review of the source code. To perform substantive testing, auditors must have an understanding of the tools used to develop and maintain RPA. This will be helpful when auditors review logs, configuration controls, privileged access controls and the like. General IT controls are applicable as always.

Conclusion

Emerging technologies bring opportunities to organizations, but they also expose the enterprise to new risk. Auditors are expected to identify the right balance between cost and benefit of internal controls for mitigating these risk factors. This includes understanding how technology integrates with business, how it is governed, which activities are automated and how they are controlled, what the business impacts are as a result of this automation, and how negative impacts are controlled and monitored. Though auditors are not expected to be experts in every technology, they should be able to identify the risk inherent with these technologies. This includes understanding the technology architecture, the internal control framework embedded in the technology and its integration with business.

Endnotes

1 PricewaterhouseCoopers (PwC), "Re-Inventing Internal Controls in the Digital Age," April 2019, *https://www.pwc.com/sg/en/publications/assets/reinventing-internal-controls-in-the-digital-age-201904.pdf*

2 Fremantle, P.; F. Leymann; S. Perera; J. Jenkins; "Emerging Technology Analysis Canvas," October 2018, *https://www.researchgate.net/publication/328172070_Emerging_Technology_Analysis_Canvas_ETAC*

3 PricewaterhouseCoopers, "Internal Audit Takes on Emerging Technologies," 2012, *https://www.pwc.com/mt/en/publications/assets/emerging_technologies.pdf*

4 Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v 4.0," 2017, *https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf*

5 The Institute of Internal Auditors, "The IIA's Artificial Intelligence Auditing Framework: Practical Applications, AI Part II," 2018, *https://na.theiia.org/periodicals/Public%20Documents/GPI-Artificial-Intelligence-Part-II.pdf*

6 The Institute of Internal Auditors, "The IIA's Artificial Intelligence Auditing Framework: Practical Applications, AI Part III," 2018, *https://na.theiia.org/periodicals/Public%20Documents/GPI-Artificial-Intelligence-Part-III.pdf*

7 Forrester, "Predictions 2020," *https://go.forrester.com/predictions*

8 Protiviti, "The Internet of Things—What Is It and Why Should Internal Audit Care?" 2016, *https://www.protiviti.com/sites/default/files/united_states/insights/internal-audit-and-the-internet-of-things-whitepaper-protiviti.pdf*

9 Boeckl, K.; *et al.*; "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," June 2019, *https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf*

10 ISACA®, Blockchain Preparation Audit Program, *https://next.isaca.org/bookstore/audit-control-and-security-essentials/wapbap*

11 Deloitte, "Auditing the RPA Environment," March 2018, *https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-auditing-the-rpa-environment-noexp.pdf*