



# EMERGING TECHNOLOGIES, RISK, AND THE AUDITOR'S FOCUS

A RESOURCE FOR AUDITORS,  
AUDIT COMMITTEES, AND MANAGEMENT

## **ABOUT THE CENTER FOR AUDIT QUALITY**

The Center for Audit Quality (CAQ) is an autonomous public policy organization dedicated to enhancing investor confidence and public trust in the global capital markets. The CAQ fosters high-quality performance by public company auditors; convenes and collaborates with other stakeholders to advance the discussion of critical issues that require action and intervention; and advocates policies and standards that promote public company auditors' objectivity, effectiveness, and responsiveness to dynamic market conditions. Based in Washington, DC, the CAQ is affiliated with the American Institute of CPAs.

*Please note that this publication is intended as general information and should not be relied upon as being definitive or all-inclusive. As with all other CAQ resources, this is not authoritative, and readers are urged to refer to relevant rules and standards. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The CAQ makes no representations, warranties, or guarantees about, and assumes no responsibility for, the content or application of the material contained herein. The CAQ expressly disclaims all liability for any damages arising out of the use of, reference to, or reliance on this material. This publication does not represent an official position of the CAQ, its board, or its members.*

# **EMERGING TECHNOLOGIES, RISK, AND THE AUDITOR'S FOCUS**

## **A RESOURCE FOR AUDITORS, AUDIT COMMITTEES, AND MANAGEMENT**

# INTRODUCTION

Emerging technologies are altering the financial reporting environment substantially, and this change is accelerating. For example, artificial intelligence (AI), robotic process automation, and blockchain are changing the way business gets done, and auditors are leading by transforming their own processes.

In this evolving environment, it is more important than ever for the key players in financial reporting—auditors, audit committees, and management—to have a strong grasp of roles and responsibilities. As the use of emerging technologies in the financial reporting process increases, it becomes less likely auditors can design traditional substantive tests (e.g., test of details or substantive analytical procedures) that, by themselves, would provide sufficient appropriate audit evidence that respond to

identified assertion-level risks.<sup>1</sup> This evolution in the sufficiency and source of audit evidence puts further emphasis on management's internal control over financial reporting.

What are key technology risks to watch for? What are auditors focusing on when it comes to the impact of emerging technologies on business? How are auditors evaluating whether management is properly assessing the impact of emerging technologies on internal control over financial reporting?

This publication sheds light on these questions, with an eye on key technology developments: the internet of things (IoT), AI, and smart contracts. This resource builds on the Center for Audit Quality's 2018 publication *Emerging Technologies: An Oversight Tool for Audit Committees*.<sup>2</sup>

<sup>1</sup> See Public Company Accounting Oversight Board (PCAOB) Auditing Standard (AS) 2301.17: The Auditor's Responses to the *Risks of Material Misstatement*, available at <https://pcaobus.org/Standards/Auditing/Pages/AS2301.aspx>.

<sup>2</sup> Available at <https://www.thecaq.org/emerging-technologies-oversight-tool-audit-committees/>.

# EMERGING TECHNOLOGIES

## RISK ASSESSMENT AND THE AUDIT

Emerging technologies can bring great benefits, but they also come with a varied set of substantial risks. (See box, “Examples of Technology Risks.”)

A core strength of the auditing profession is the assessment of risks and controls. As they address the challenge of assessing technology risk, auditors can and should focus on the following:

**1. Auditors should gain a holistic understanding of changes in the industry and the information technology environment to effectively evaluate management’s process for initiating, processing, and recording transactions and then design appropriate auditing procedures.**

This understanding includes, but is not limited to, understanding likely sources of potential misstatements and identifying risks and controls within information technology.

These are integral procedures of the top-down approach auditors use to identify significant accounts and disclosures and their relevant assertions during the risk assessment process.<sup>3</sup>

**2. Auditors, as appropriate, should consider risks resulting from the implementation of new technologies and how those risks may differ from those that arise from more traditional, legacy systems.**<sup>4</sup> Auditors should be aware risks can arise due to program or application-specific circumstances (e.g., resources, rapid tool development, use of third parties) that could differ from traditional IT implementations. Understanding the system development lifecycle risks introduced by emerging technologies will help auditors develop an appropriate audit response tailored to an organization’s circumstances.

<sup>3</sup> See PCAOB AS 2110: *Identifying and Assessing Risks of Material Misstatement*, available at <https://pcaobus.org/Standards/Auditing/Pages/AS2110.aspx>.

<sup>4</sup> See PCAOB AS 2201.09: *An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements*, available at <https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx>.

**3. Auditors should consider whether specialized skills are necessary to determine the impact of new technologies and to assist in the risk assessment and understanding of the design, implementation, and operating effectiveness of controls.**<sup>5</sup> If specialized skills are considered appropriate, auditors may seek the involvement of a subject matter expert. Auditors also should obtain a sufficient understanding of the expert's field of expertise to evaluate the adequacy of the work for that auditor's purposes.<sup>6</sup>

### EXAMPLES OF TECHNOLOGY RISKS

- + Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both
- + Unauthorized access to data that might result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions (specific risks might arise when multiple users access a common database)
- + The possibility of information technology personnel gaining access privileges beyond those necessary to perform their assigned duties, thereby leading to insufficient segregation of duties
- + Unauthorized or erroneous changes to data in master files
- + Unauthorized changes to systems or programs
- + Failure to make necessary or appropriate changes to systems or programs
- + Inappropriate manual intervention
- + Potential loss of data or inability to access data as required<sup>7</sup>
- + Risks introduced when using third-party service providers
- + Cybersecurity risks applicable to the audit<sup>8</sup>

<sup>5</sup> See PCAOB AS 1210.06: *Using the Work of a Specialist*, available at <https://pcaobus.org/Standards/Auditing/Pages/AS1210.aspx>.

<sup>6</sup> See PCAOB AS 1210.09.a: *ibid.*

<sup>7</sup> See PCAOB AS 2110.B4: *ibid.*

<sup>8</sup> See CAQ, *Understanding Cybersecurity and the External Audit*, available at [https://www.thecaq.org/wp-content/uploads/2019/03/cybersecurity\\_and\\_external\\_audit\\_final.pdf](https://www.thecaq.org/wp-content/uploads/2019/03/cybersecurity_and_external_audit_final.pdf).

# TECHNOLOGY IMPACT

## POTENTIAL AREAS OF AUDITOR FOCUS

### HOW TECHNOLOGY AFFECTS A COMPANY'S BUSINESS

As auditors obtain an understanding of management's implementation and oversight of new technologies, they also will perform procedures to understand the changes to the company's business, including any changes to the information technology environment. Areas of focus could include understanding the following:

- + New activities or changes to existing processes due to new technology (e.g., new revenue streams, changes in the roles and responsibilities of entity personnel, automation of manual tasks, changes in staffing levels that affect an entity's internal control environment)
- + Changes in the way the entity's systems are

developed and maintained (e.g., by moving from a traditional waterfall<sup>9</sup> development approach to a more agile development framework<sup>10</sup>) and whether these changes introduce new risks and require new controls to respond to those risks

- + The impact the new technology has on how the organization obtains or generates and uses relevant, quality information to support the functioning of internal control

### HOW TECHNOLOGY AFFECTS INTERNAL CONTROLS OVER FINANCIAL REPORTING

Auditors will perform procedures to understand the steps management is taking to evaluate how the new technology is impacting the company's system of internal control. To obtain this

<sup>9</sup> Waterfall is a linear approach to software development. See Mary Lotz, "Waterfall vs. Agile: Which Is the Right Development Methodology for Your Project?" Available at <https://www.seguetech.com/waterfall-vs-agile-methodology/>.

<sup>10</sup> Agile is an iterative, team-based approach to development. *ibid.*

**“TO BE MOST EFFECTIVE AS TECHNOLOGY AROUND FINANCIAL REPORTING AND AUDITING CONTINUES TO EVOLVE, STAKEHOLDERS—INCLUDING INVESTORS, PREPARERS, BOARDS, AUDIT COMMITTEES, AUDITORS, REGULATORS, AND ACADEMICS—SHOULD ACTIVELY PARTICIPATE IN THAT DEVELOPMENT, SHARING THEIR UNIQUE PERSPECTIVES. WHY? THAT WAY WE CAN BETTER ENSURE INNOVATION AND GROWTH THAT MAXIMIZES VALUE FOR INVESTORS AND THE ECONOMY IN A SAFE AND SUSTAINED MANNER.”**

**Kathleen Hamm**

**Board Member, Public Company Accounting Oversight Board  
Remarks before the 43rd World Continuous Auditing & Reporting  
Symposium, November 2, 2018**

understanding, auditors may ask management about the following areas:

- + The impact the new technology has on the organization's identification and assessment of risks relevant to the achievement of control objectives
- + The impact the new technology has had or should have had on the entity's internal controls over financial reporting (ICFR)
- + The sufficiency of the design of information technology general controls to address the identified risks
- + Management's risk assessment process and whether it considers all applicable information technology systems where control activities are occurring, including, but not limited to:
  - upstream/downstream data interfaces, and
  - systems used by outsourced service providers and other business partners

- + Whether indirect effects of new technology have been appropriately considered and addressed (e.g., staffing levels, competency of internal personnel, access to appropriate resources, cybersecurity risks as applicable to the audit)
- + Whether the nature of the technology impacts the fraud risk assessment, including the risks of material misstatement to the financial statements due to fraud and the risk of misappropriation of assets (both monetary and nonmonetary)

### **HOW TECHNOLOGY AFFECTS AUDIT COMMITTEE OVERSIGHT OF FINANCIAL REPORTING**

Auditors also will be interested in how the audit committee is overseeing the impact of emerging technologies on financial reporting, including the following:

- + The level of oversight over the entity's financial reporting process and ICFR, including relevant risks and controls related to emerging technologies

- + The level of involvement of the internal audit function
- + The communication protocols in place for the audit committee to obtain information to effectively carry out its responsibilities, which may require the managers of large technology projects to present their progress periodically to the audit committee. Auditors may consider it appropriate to attend such presentations. •

### KEY STEPS FOR AUDITORS IN A CHANGING TECHNOLOGY ENVIRONMENT

As auditors obtain an understanding of the impact of technology on a company's business, its systems of internal control, and its financial reporting, some important reminders include the following:

- + **Maintain sufficient professional skepticism** when reviewing management's risk assessment for new systems.
- + **Understand the direct and indirect effects of new technology** and determine how its use by the entity impacts the auditor's overall risk assessment.
- + **Understand how the technologies impact the flow of transactions**, assess the completeness of the in-scope ICFR systems, and design a sufficient and appropriate audit response.
- + **Assess the appropriateness of management's processes** to select, develop, operate, and maintain controls related to the organization's technology based on the extent the technology is used. •



# KEY TECHNOLOGY DEVELOPMENTS

## THE BASICS AND AUDITOR IMPLICATIONS

The following are emerging technology developments that illustrate the impact technology can have on planned audit procedures, often requiring auditors to understand and perform procedures on a larger group of systems that produce information relevant to the production of financial statements.

Based on management's and auditors' independent risk assessment procedures, the audit's scope may need to include peripheral systems, as well as testing general IT and application controls relative to those systems due to the increased use of technology that is relevant to financial reporting.

### INTERNET OF THINGS AND PERIPHERAL SYSTEMS

#### The Basics

In essence, IoT is the concept of connecting any device (cell phones, coffee makers, washing

machines, and so on) to the internet, each other, and other devices. This concept also applies to components of machines (e.g., a jet engine or the drill of an oil rig). Research firm Gartner predicts that there will be over 26 billion connected devices by 2020.<sup>11</sup>

#### Auditor Implications

A shift to connected devices and systems may result in auditors not being able to rely only on manual controls. Instead, auditors may need to scope new systems into their audit. Audit firms may need to train auditors to evaluate the design and operating effectiveness of automated controls.

Consumer-facing tools that connect to business environments in new ways can impact the flow of transactions and introduce new risks for management and auditors to consider. Consider payment processing tools that allow users to pay

<sup>11</sup> See, Jacob Morgan, "A Simple Explanation of 'The Internet of Things,'" available at <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7d647c481d09>.

via credit card at a retail location through a mobile device. This could create a new path for incoming payments that may rely, in part, on a new service provider supplying and routing information correctly.

Another potential scenario is a refrigerator that monitors food and beverage usage and supply at an individual consumer level and could execute orders and payments via an internet connection. Auditors would need to consider the volume of those transactions and the processes and controls related to whether those transactions flow similarly to other e-commerce at an organization or have unique considerations.

### AI USED IN MONITORING BUSINESS OPERATIONS

#### The Basics

AI tools use advanced algorithms and machine learning to predict activity and manage business processes, such as projecting inventory levels, managing cash flow needs, or by enhancing monitoring and other activities in internal audit.

#### Auditor Implications

Using AI tools to drive business decisions (e.g., how much inventory to buy, how much cash to draw down) does not necessarily introduce new audit risks because business changes can create operational risks that are not necessarily audit risks. However, auditors should confirm their understanding of how the use of AI affects the entity's flows of transactions, including the generation of reports or analytics used by management. Auditors also should consider whether the AI is making decisions—or being utilized by management as part of the decision-making process.

When AI is deployed in monitoring through predictive analytics that narrow management's focus on specific items or through the identification of specific reconciling activities within a population, auditors need to understand where that reliance exists and whether other controls over those activities exist. If internal audit shifts its focus on oversight by relying on AI, auditors should understand what shift occurred, how new risks might be addressed, and whether existing risks may not be getting the same level

of attention. Understanding these changes could drive changes in the audit approach.

### SMART CONTRACTS

#### The Basics

Certain blockchains offer the ability to execute smart contracts. A smart contract is computer code running on top of a blockchain containing a set of rules in which the parties to the contract agree to interact with each other. When predefined rules are met, the agreement is automatically executed by the computer code. The smart contract code facilitates, validates, and enforces the performance of an agreement or a transaction. Examples of smart contracts include the following:

1. A retail organization might engage in smart contracts with its suppliers. Under the smart contracts, goods could be rejected when predefined criteria are met. For example, IoT devices could check the temperature of perishable products during transportation—the smart contract will automatically reject shipments that have had temperature variations outside of a predefined threshold.
2. A bank or a title company might enter into a transaction to exchange cash for real property. Rather than escrows and deed exchanges, a smart contract could execute the delivery of cash (via digital tokens) automatically upon the receipt of a deed that has been tokenized on the blockchain.

#### Auditor Implications

Auditors will want to develop an understanding of where smart contracts are used and whether the smart contract affects an entity's financial reporting. If the smart contract performs checks that could be deemed a key control within the system of ICFR, then additional testing may need to be performed.

### AI'S POTENTIAL USE IN DEVELOPING ACCOUNTING ESTIMATES

#### The Basics

AI may be used in developing accounting estimates and potentially could incorporate data previously determined to not be relevant into the overall

development of the estimate. AI may identify correlations in the data that were previously unknown.

Take the example of using AI to develop an allowance for loan and lease losses (ALLL). In addition to looking at traditional inputs regarding delinquencies and the relationship to FICO scores, the AI may notice other correlations among the data elements that could impact the ALLL calculation, such as certain macro-economic factors that may not have previously been considered in determining the ALLL. If entity management historically was not including those data elements as relevant to the ALLL model, new risk identification and response processes and procedures would need to be developed to evaluate the completeness, accuracy, and appropriateness of inclusion of those factors.

### **Auditor Implications**

As part of testing the accounting estimate, auditors would consider the more traditional risks related to the completeness and accuracy of the data elements, as well as the AI's methodology, which may present unique challenges due to the machine learning inherent in AI.

# CONCLUSION

While emerging technologies can bring about great opportunities and efficiencies for a business, they also bring with them new challenges. An understanding of these emerging technologies and an awareness of the benefits and risks they present to financial reporting is essential for auditors, management, and audit committees to discharge their respective responsibilities. •

# WE WANT TO HEAR FROM YOU

So that we can provide resources that are informative and best address the needs of our stakeholders, we would appreciate your response to **three** short questions.

**CLICK FOR SURVEY**

SURVEY LINK: [http://thecaq.qualtrics.com/jfe/form/SV\\_abKdNA73JXmdkWh](http://thecaq.qualtrics.com/jfe/form/SV_abKdNA73JXmdkWh)

**EMERGING  
TECHNOLOGY  
RISK, AND  
AUDITOR'S**

**A RESOURCE FOR AU  
AUDIT COMMITTEES,**

**G  
OLOGIES,  
D THE  
S FOCUS**

**EDITORS,  
AND MANAGEMENT**



Published May 2019

**THECAQ.ORG**

**WE WELCOME  
YOUR FEEDBACK**

Please send comments  
or questions to  
[info@thecaq.org](mailto:info@thecaq.org)