CCH® PUBLICATIONS

Top Accounting and Auditing Issues for 2024 CPE Course

BONUS CPE COURSE!

Earn CPE Credit and stay on top of key accounting and auditing issues. Go to CCHCPELink.com/printcpe

Wolters Kluwer

Top Accounting and Auditing Issues for 2024 | CPE Course

Salvatore A. Collemi, CPA
Lynn Fountain, CPA, CGMA, CRMA
Robert K. Minniti, CPA, CFE, CrFA, CVA, CFF, MAFF, CGMA, PI, DBA

Wolters Kluwer

Contributors

Contributing Editor . . . . . Salvatore A. Collemi, CPA

Lynn Fountain, CPA, CGMA, CRMA

Robert K. Minniti, CPA, CFE, CrFA, CVA, CFF, MAFF, CGMA, PI, DBA

Production Coordinator . . . . . Mariela de la Torre; Jennifer Schencker;

Gokiladevi Sashikumar; Leila Taylor

Production . . . . . Sharon Sofinski; Anbarasu Anbumani

2700 Lake Cook Road
Riverwoods, IL 60015
800 344 3734
CCHCPELink.com

Introduction

Top Accounting and Auditing Issues for 2024 CPE Course helps CPAs stay abreast of the most significant new accounting and auditing standards and important projects. It does so by identifying the events of the past year that have developed into hot issues and reviewing the opportunities and pitfalls presented by these changes. The topics reviewed in this course were selected because of their impact on financial reporting and because of the role they play in understanding the accounting and auditing landscape in the year ahead.

Module 1 of this course reviews top accounting issues.

Chapter 1 introduces the topic of Environmental, Social, and Corporate Governance (ESG) and what accountants and management should know.

Chapter 2 addresses the most frequently asked questions, specific risks, and challenges emerging in properly accounting for and auditing digital assets.

Chapter 3 addresses how criminals take advantage of employees to commit data breaches or to place malware on an organization's computers. It also discusses cyber fraud awareness training and internal controls to help prevent these types of fraud.

Module 2 of this course reviews top auditing issues.

Chapter 4 walks through the key areas of the new requirements surrounding the auditor's report. The auditor's report, while maintaining a good amount of the extant language, will be expanded as a result of the new standards.

Chapter 5 is designed to provide external auditors with practical and insightful perspectives on how to audit transactions under the Financial Accounting Standards Board (FASB) Accounting Standards Codification (ASC) Topic 842, *Leases*. Topics addressed include the new accounting and financial reporting requirements and how to substantively and analytically test them in accordance with professional standards.

Chapter 6 discusses what the future holds for internal auditors. Topics covered include how to address challenges and emerging risks, and the importance of staying relevant, being proactive, upgrading skills, and understanding the role of technology. It also briefly discusses the Institute of Internal Auditors proposed *Global Internal Audit Standards* that will replace the International Professional Practices Framework for internal auditors.

Study Questions. Throughout the course you will find Study Questions to help you test your knowledge, and comments that are vital to understanding a particular strategy or idea. Answers to the Study Questions with feedback on both correct and incorrect responses are provided in a special section beginning at ¶ 10,100.

Final Exam. This course is divided into two Modules. Take your time and review all course Modules. When you feel confident that you thoroughly understand the material, turn to the Final Exam. Complete one or both Final Exams for continuing professional education credit.

Go to **cchcpelink.com/printcpe** to complete your Final Exam online for immediate results. My Dashboard provides convenient storage for your CPE course Certificates. Further information is provided in the CPE Final Exam instructions at ¶ 10,300. **Please note, manual grading is no longer available for Top Accounting and Auditing Issues. All answer sheets must be submitted online for grading and processing.**

September 2023

PLEDGE TO QUALITY

Thank you for choosing this CCH® CPELink product. We will continue to produce high quality products that challenge your intellect and give you the best option for your Continuing Education requirements. Should you have a concern about this or any other Wolters Kluwer product, please call our Customer Service Department at 1-800-344-3734.

COURSE OBJECTIVES

This course provides an overview of important accounting and auditing developments. At the completion of this course, the reader will be able to:

- Identify the concepts and each component of ESG
- Identify a framework for ESG
- Determine the ESG responsibilities of accountants, management, and the board of directors
- Identify various accounting considerations related to ESG
- Identify ESG impacts on financial reporting and disclosure controls and procedures (DCP)
- Recognize how to measure ESG performance
- Identify how to answer frequently asked questions related to the fair presentation and disclosure of cryptocurrency and other digital assets
- Recognize common risks associated with these instruments and how to properly audit them
- Identify phishing, vishing, and smishing
- Recognize common cyber fraud schemes
- Identify internal controls to help prevent and detect cyber frauds
- Identify the new requirements of the reporting under the AICPA's *Professional Standards*
- Recognize the new form and content of the updated auditor's report and when and how to modify it
- Identify the Statement on Auditing Standards (SAS) that was issued in May 2019 to improve the transparency and relevance of the communication in the auditor's report
- Identify a characteristic/change with respect to SAS No. 134
- Identify the type of audit of an employee benefit plan that used to be called a "limited scope audit" that will now be referred to as an "ERISA Section 103(a)(3)(C)" audit, subsequent to the release of SAS No. 136
- Explain the key auditing concept addressed by SAS No. 138
- Recognize the FASB's new leasing standard requirements
- Describe the new accounting and reporting requirements of leases
- Identify which audit procedures to perform
- Explain how to properly audit the transition requirements and initial adoption of the new leasing standard

- Identify approximately what amount of right-of-use (RoU) assets and lease payment liabilities will be added on by U.S. companies' balance sheets on account of the new lease standard
- Identify the ASU issued by the FASB on June 2, 2020, that amended the effective date of the new leasing standard
- Identify a contract, or part of a contract, that conveys the right to control the use of identified property, plant, or equipment for a period of time in exchange for consideration
- List the types of costs that are commissions or payments made to an existing tenant to terminate the lease
- Explain the context of the proposed *Global Internal Audit Standards*
- Identify the challenges for auditors to stay relevant in a changing business environment
- Identify challenges to the traditional audit process
- Identify top emerging risks for internal audit
- Explain how to evaluate the impact of the changing environment (due to COVID-19) on the work plan of internal audit
- Identify and examine actions internal audit can take to address challenges
- Recognize the importance of upgrading the skills and exposure of the internal audit team
- Recognize the role of technology in assuring a smooth transition to value-added auditing

---

Additional copies of this course may be downloaded from **cchcpelink.com/printcpe**. Printed copies of the course are available for $15.00 by calling 1-800-344-3734 (ask for product 10024493-0011).

Contents

MODULE 1: TOP ACCOUNTING ISSUES—CHAPTER 1: Introduction to Environmental, Social, and Governance (ESG) for Accountants

¶ 101 WELCOME

Environmental, Social, and Corporate Governance (ESG) refers to the factors in measuring the sustainability and societal impact of an investment in a company or business. Analysis of these criteria can help determine the future financial performance of companies. This chapter introduces the topic of ESG and what accountants and management should know.

¶ 102 LEARNING OBJECTIVES

Upon completion of this chapter, you will be able to:

- Identify the concepts and each component of ESG
- Identify a framework for ESG
- Determine the ESG responsibilities of accountants, management, and the board of directors
- Identify various accounting considerations related to ESG
- Identify ESG impacts on financial reporting and disclosure controls and procedures (DCP)
- Recognize how to measure ESG performance

¶ 103 WHAT IS ESG?

ESG criteria are a set of standards for a company's operations that today's socially conscious investors use to screen potential investments. The standards include three central factors measuring the sustainability and society impact of an investment:

- **Environmental** criteria look at how a company performs as a steward of nature in protecting the planet.
- **Social** criteria examine how the company manages relationships with employees, suppliers, customers, and the communities where it operates.
- **Governance** deals with a company's leadership, the pay of its executives, audits, internal controls, and shareholder rights. ESG analysts seek to understand how leadership's incentives are aligned with stakeholder expectations, how shareholder rights are viewed and honored, and what types of internal controls exist to promote transparency and accountability on the part of leadership.

ESG is one of the new ways investors evaluate companies. Investors demand enhanced information about how companies are approaching environmental sustainability. The foundation of sustainability reporting is for an organization to identify and prioritize its impacts on the economy, environment, and people—to be transparent about their impacts.

An ESG score is an objective measurement or evaluation of a company, fund, or security's performance with respect to ESG issues. A 2020 survey by a company called SustainAbility (https://www.sustainability.com/globalassets/sustainability.com/thinking/pdfs/sustainability-ratetheraters2020-report.pdf) found that ESG ratings are the most frequently referenced source of information that institutional investors rely on to gauge ESG performance (55 percent, tied with direct company engagement). Another survey found that 88 percent of investment professionals use third-party ESG ratings as a part of their investment process, and that 92 percent are expected to do so in the future. It is very clear that ESG is now an important issue for investors.

ESG risks involve issues such as energy efficiency, worker safety, and board independence. The risks have financial implications but are often not highlighted during traditional financial reviews.

ESG Ratings Firms

The ESG ratings industry is highly fragmented, with dozens of ratings agencies and data providers in existence. The backgrounds of these firms are not uniform; many entered the ESG ratings business from different areas of expertise. Examples of ESG ratings firms include the following:

- MSCI (an American finance company that is a global provider of equity, fixed income, real estate indexes, multi-asset portfolio analysis tools, and ESG and climate products) publishes ESG ratings on 8,500 companies (14,000 issuers) globally.
- ISS ESG (the responsible investment arm of Institutional Shareholder Services Inc., the world's leading provider of environmental, social, and governance solutions for asset owners, asset managers, hedge funds, and asset servicing providers) publishes ratings on 11,800 issuers and 25,000 funds. It is a subsidiary of the largest proxy advisory firm that provides recommendations to investment management firms on how to vote on proxy issues.
- Sustainalytics (a company that rates the sustainability of listed companies based on their environmental, social, and corporate governance performance) publishes ESG ratings on over 13,000 companies.
- Refinitiv (the rebranded data provider Thomson Reuters) calculates ESG scores on 11,800 companies.
- FTSE Russell (a subsidiary of the London Stock Exchange Group that produces, maintains, licenses, and markets stock market indices) publishes ratings on 7,200 securities.

NOTE: Key questions that should be asked about ESG are:

- How is information used to assess risk and reward, and manage effectiveness?
- How do stakeholder expectations influence corporate action?
- What are key concerns for corporations/investors?

Why Is ESG Important?

The metrics related to the percentage of U.S. public companies that include some form of environmental or social metrics as part of their executive incentive plans varies widely. Per a report from the Conference Board in October 2022, the vast majority of S&P 500 companies are now tying executive compensation to some form of ESG performance. This number has grown from 66 percent in 2020 to 73 percent in 2021.The most significant increase was found in companies' use of diversity, equity, and inclusion (DEI) goals, rising from 35 percent in 2020 to 51 percent in 2021, as investors and other

stakeholders continue to focus on diversity—making it a priority for companies as well. For example, in 2022, U.S. Mastercard said that it would tie bonuses for its senior executives to three factors: reducing the company's carbon usage, building financial inclusion, and improving gender pay parity. In April 2022, Mastercard's CEO announced that the company would offer sustainability-linked pay to all employees, noting: "Each and every one of us shares the responsibility to uphold our ESG commitments. That's why we're extending that model to our annual corporate score and all employees globally, taking our shared accountability and progress to the next level."

In February 2022, COSO (the Committee of Sponsoring Organizations of the Treadway Commission) approved a study to develop supplemental guidance and insights to its authoritative 2013 Internal Control Framework in the areas of sustainability and ESG. The goal is to help all organizations create and ensure effective internal control. This should be done by applying internal controls over financial reporting (ICFR) to sustainability reporting for internal decision-making and external public reporting (both voluntary and mandated by regulators).

ESG History and Future

In the 1980s, environment, health, and safety (EHS) efforts were centered on the development of environmental and employee health regulations. The 1990s saw a shift in focus toward sustainability and reducing environmental impacts beyond legal requirements. From 2000 through the 2010s, corporate social responsibility (CSR) and corporate philanthropy/volunteerism were key strategies that companies highlighted on their websites and included as part of their media plans. Since 2020, there has been an increased focus on corporate disclosures and transparency to investors, creditors, and stakeholders.

In the future, the following key factors will affect ESG's growth into mainstream corporate accountability:

- Materiality of ESG issues and their influence on investor risk and returns
- Transparency and greater clarity on how client money is invested
- Regulation, both national and international threats (e.g., climate change)

¶ 104 DISSECTING ESG

This section describes the three components of ESG—environmental, social, and governance—in more detail.

Environmental

Climate change is a true risk to businesses, and therefore one of the most significant concerns of ESG is the environment. Investors are demanding enhanced information about how companies are approaching environmental sustainability, often referred to as *sustainability accounting*. The foundation of sustainability reporting is for organizations to identify and prioritize their impacts on the economy, environment, and people—and to be transparent about those impacts.

The environment has been a focus of investors and stakeholders for many years. As of 2021, climate risk was the most relevant ESG factor for the decision-making of institutional investors worldwide. In a 2021 survey conducted by Statista (an organization that provides data analysis, data management, statistics, data mining, machine learning, text analytics, and data visualization procedures), 79 percent of the respondents stated that environmental issues are a top risk or opportunity factor in their view. Environmental issues span far and wide, relating to a multitude of areas, some of which are described below.

Global warming. Climate change refers to long-term shifts in temperature and weather patterns. Since the 1800s, human activities have been the main driver of climate change. This is primarily due to the burning of fossil fuels (e.g., coal, oil, and gas), which produces greenhouse gases, trapping heat in the atmosphere.

Pollution. Environmental pollution is the contamination of physical and biological components of the earth and its atmosphere. Contamination is the impact to such an extent that normal environmental processes become adversely affected.

Sustainability. Environmental sustainability is the responsibility (related to the planet) to maintain natural resources and avoid adversely impacting the ability of future generations to meet their needs.

Waste reduction. This is the practice of using less material and energy to minimize waste generation and preserve natural resources. Waste reduction is broader than recycling, because it incorporates ways to prevent materials from ending up as waste before they reach the recycling stage. A key part of waste "reduction" is "conservation." This means using natural resources wisely and using them to avoid waste.

Deforestation. Deforestation, or forest clearance, is the removal of a forest or strand of trees from land that is then converted to non-forest use. It can involve the conversion of forest land to farms, ranches, or urban use.

Desertification. Desertification is a type of land degradation in drylands. Biological productivity is lost due to natural processes introduced by human activities, resulting in fertile areas becoming increasingly dry.

Rapid population growth. The combination of a continuing high birth rate and low death rate is creating a rapid population increase in many countries. This type of growth is seen in Asia, Latin America, and Africa, where people generally live longer.

Food protection and equitable distribution. Food protection and equitable distribution incorporates processes from farm to table and from processing to disposal. This system ensures economic opportunity; high-quality jobs with living wages; access to healthy, affordable food; and environmental sustainability and safe working conditions.

Depletion of the atmospheric ozone. Ozone depletion is the gradual thinning of the Earth's ozone layer in the upper atmosphere. It is caused by the release of chemical compounds containing gaseous outputs (chlorine or bromine) from industry and other human activities.

- Chlorine is the second lightest of the halogens. It appears between fluorine and bromine in the periodic table and its properties are mostly intermediate between them.
- Bromine is a volatile red-brown liquid at room temperature that evaporates readily to form a similarly colored vapor. Its properties are intermediate between those of chlorine and iodine.

Acid precipitation and air pollution. These are caused by a chemical reaction that begins when compounds are released into the air. Substances rise high into the atmosphere, where they react with water, oxygen, and other chemicals to form more acidic pollutants.

Ocean pollution. This type of pollution occurs when substances used by humans enter the ocean and cause harmful effects. Ocean-polluting elements include industrial, agricultural, and residential waste; particles; noise; excess carbon dioxide; and invasive organisms.

EXAMPLE: One of the largest environmental disasters in American history, the 2010 British Petroleum (BP) Deepwater Horizon oil spill released an estimated

4.9 million barrels of oil into the Gulf of Mexico, making it the largest marine oil spill in the history of the petroleum industry. The well was eventually declared "sealed" in September 2010, and for its role in the disaster, BP ended up paying $53.8 billion in fines, cleanup costs, and local reparations.

Social

At its core, the social component of ESG is about human rights and equity. It encompasses an organization's relationships with people, as well as its policies and actions that affect individuals, groups, and society. Related issues include geopolitical events, labor issues, safety risks, and social dynamics.

An example of the social component relates to geopolitical events that can prevent companies from producing and distributing their products. Another example is when an international political conflict (e.g., Russian sanctions) threatens the stability of organizations.

EXAMPLE: A 2021 drone attack on an oil refiner in Saudi Arabia temporarily halted 5 percent of worldwide oil production.

Analyses of these events involve questions around the likelihood of prolonged conflict. According to the S&P Global Ratings Segment, oil and gas companies tend to have high exposure to social factors in all ESG categories (not just environmental) due to the serious damage accidents or changes in government policy can do to a company's performance across various indicators.

Social factors to consider in sustainable investing also include a company's strengths and weaknesses in dealing with social trends, labor, and politics. Often the impacts of labor disputes on a business can be an example (e.g., striking workers).

EXAMPLE: In August 2021, S&P Global Market Intelligence reported that the retailer Kohl's hired its seasonal workers two months earlier than usual because of the tightening labor market. Due to the social issues at play, the company anticipated having difficulty in maintaining its workforce and took action.

Safety risks come with the safety implications of a product or politics of the company's supply chain. Companies that ensure their products and services are safe and/or minimize the exposure to geopolitical conflicts in their supply chains will face less volatility in their businesses than those that do not. Also, companies should keep in mind that social dynamics are created from surges in online public opinion. Material on social media can go viral and affect a company's reputation in an instant.

Governance

In today's world, all stakeholders expect companies to ethically manage their businesses. Stakeholders are interested in how companies address governance processes, including business ethics, risk management, and legal compliance.

The *G* in ESG refers to the governance factors of decision-making. This extends from sovereigns' policymaking to the distribution of rights and responsibilities among different participants in corporations, including the board of directors, managers, shareholders, and stakeholders. Governance factors allow investors to screen for appropriate governance practices as they would for environmental and social factors, for example:

- A corporation's purpose,
- The role and makeup of boards of directors,
- Shareholder rights, and
- How corporate performance is measured.

These are all core elements of corporate governance structures. S&P Global assesses companies' governance performance by assessing four factors: (1) the structure and oversight of the organization, (2) its code of conduct and values, (3) its transparency and reporting, and (4) its cyber risk and systems.

There are varying opinions on which interests should be prioritized in decision-making. One view is to maximize financial returns for shareholders. This assumes maximizing returns is the purpose of companies' operations. Another view is that stakeholders deserve more importance and support over profit-making.

EXAMPLE: According to SPG Global, in August 2019, more than 180 CEOs of major corporations declared as part of the business roundtable that companies should concentrate on providing benefits to all stakeholders alongside deriving profits for shareholders. Sustainability-focused groups called on leaders like these to take further actions that benefit customers, employees, and communities along with shareholders.

Gender diversity and equity—also known as diversity, equity, and inclusion (DEI)—is another governance issue. One aspect relates to shareholders demanding better representation of women and minorities on corporate boards and in executive ranks. This includes equal compensation and mobility for women and people of color.

As part of their DEI efforts, more companies are emphasizing the financial benefit of creating inclusive workplaces in an effort to increase diversity and inclusivity. In fact, S&P Global Market Intelligence research revealed that firms with more women on their board of directors and in C-suite positions had greater financial performance than less diverse companies.

Another element of governance is compensation and oversight of CEOs and top executives relating to the structure and makeup of boards. Regulators in the United States and United Kingdom require publicly traded companies to allow shareholders to vote on executive compensation packages at regular intervals. In the United States, companies may be required to annually disclose the ratio of CEO-to-median-employee pay. However, multiple elements of the processes for selecting, evaluating, and rewarding top executives remain unregulated. This leaves an organization's board of directors responsible for this key component of a company's corporate governance.

EXAMPLE: Companies like We Work (a provider of coworking spaces, including physical and virtual shared spaces, headquartered in New York) have been scrutinized for their lack of leadership accountability, oversight, and conflicts of interest. Critics point to the lack of basic internal controls, including inadequate oversight of their CEOs and other senior executives. These are seen as corporate governance flaws.

The governance component of ESG is critical, as governance risks and opportunities will most likely increase as social, political, and cultural attitudes evolve. The S&P Global Ratings ESG Evaluation examines potential environmental and social risks to determine an entity's capacity to operate successfully. In addition, it determines whether the entity is effectively managing its exposure to governance risks and opportunities.

STUDY QUESTIONS

1. Which of the following statements is correct with respect to ESG?

- **a.** ESG concepts are a set of requirements for an organization's financial statements.
- **b.** The standards include two central factors measuring sustainability.
- **c.** An ESG score is an objective measurement or evaluation of a company with respect to ESG issues.
- **d.** The ESG ratings industry is highly centralized.

2. A 2021 survey conducted by Statista indicated what percentage of respondents felt that environmental issues are a top risk or opportunity factor?

- **a.** 40 percent
- **b.** 60 percent
- **c.** 79 percent
- **d.** 85 percent

3. There are several key factors that exist in ESG's growth into mainstream corporate accountability. Which of the following is ***not*** one of these factors?

- **a.** Consistency
- **b.** Materiality
- **c.** Transparency
- **d.** Regulation

¶ 105 BENEFITS OF ESG

Now that we've covered the history of ESG and explained each of its components, it's time to consider the benefits of ESG.

Risk Reduction

ESG can help an organization identify immediate and long-term risks. The integration of ESG practices makes a company less vulnerable to reputation, political, and regulatory risk, leading to lower volatility of cash flows and profitability. Doing the right things means the company is less exposed in the long run.

Opportunity Management

Oversight of ESG in changing markets can reveal unmet needs for new products or services, unserved or underserved customer bases, and strategic relationships for addressing ESG issues. In emerging markets, ESG efforts can provide:

- Greater profitability and market penetration; and
- Positive social impact through a wide range of training and support to independent stores, kiosks, and microbusinesses.

Culture

A company's ability to embrace ESG can be an indicator of commitment to building a high-performing, purpose-driven workforce, and an inclusive culture. Integrating ESG factors into an organization's value allows greater insight into intangible factors, such as culture, talent recruitment and retention, operational excellence, and risk management—and all of these can improve investment outcomes.

Environmental Issues and Scarcity of Resources

As mentioned earlier, climate change and global warming present significant risks. An understanding of these risks allows a company to be proactive with initiatives for mitigation.

Resource scarcity occurs when demand for a natural resource is greater than the available supply. Changing environmental conditions and regulations have increased the depletion of natural resources. Therefore, conducting due diligence is critical for an organization to maintain a strong ESG presence.

Reputational Risk

ESG issues can lead to reputational risk and health concerns, which can influence a company's license to operate and result in legal and regulatory ramifications. For example, polluted beaches can have an impact on local tourism, travel, and leisure industries. Even if environmental factors do not impact a company or portfolio directly, they may have a material impact on key stakeholders, customers, consumers, and suppliers.

¶ 106 ESG PROGRAMS

ESG is used as a framework to assess how a company manages risks and opportunities that shifting market and nonmarket conditions create. This framework includes an evaluation of a company's:

1. Environmental systems,
2. Social systems, and
3. Economic systems.

Note that ESG is not about immediate values—rather, it is about the ability to create and sustain longer-term values in a rapidly changing world, and managing the risks and opportunities associated with these changes.

Those who are tasked with developing an ESG program in their organization must keep in mind that an ESG program is not a one-size-fits-all. Each organization must take a disciplined approach to identifying which elements are required within its program and which components are specific to its industry. This involves assessing the organization's needs at several levels. To establish an ESG program, a company should take the following steps:

1. Determine business-specific ESG issues.
2. Evaluate existing programs.
3. Identify gaps from the organization's current operational state.
4. Set goals and create a framework for ESG.
5. Determine reporting requirements and report progress.
6. Develop actionable plans and key performance indicators.

The demand for companies to act on ESG will only grow in the future. The global consulting firm of Korn Ferry rated sustainability as one of the seven areas dominating the future of work trends in 2022. One of its reports (https://www.kornferry.com/insights/featured-topics/future-of-work) indicated that investors, partners, customers, and employees are all turning their backs on businesses that will not commit to building a sustainable future. Korn Ferry expects that organizations will accept the reality that they need to commit to actions that transform businesses. The firm proposed a series of five questions organizations should consider:

- **Purpose.** Why are we implementing ESG? Who are we trying to satisfy? What is the time horizon? How will success be measured? Who should oversee the program?
- **Leadership and talent.** How do we attract, develop, and retain the leadership, talent, and skills needed to drive ESG strategy and outcomes?

- **Governance.** How should our board evolve to oversee, enable, and support delivery of our ESG strategy?
- **Operating model.** How do we organize to deliver our ESG and sustainability strategy? Note that companies may need to change the way they operate to meet goals.
- **Culture and mindset.** How do we create the right culture and mindsets, engage our people, and reinforce the right behaviors?

¶ 107 ESG ROLES

Considering the framework outlined earlier, what roles must the board, management, and accountants take? Armed with analytical skills, business knowledge, and the ability to understand and apply reporting standards, accountants are positioned to work in several areas when addressing ESG concerns, including reporting, cost analysis, and audit and assurance services.

The Accountant's Role

Reporting. This involves reviewing current financial systems and tracking systems that might have to be modified to incorporate ESG information. Newer enterprise resource planning systems might have a specific ESG module that can be incorporated into existing systems for reporting to the board of directors or to management.

Cost analysis. Professionals frequently analyze investments using data from analysis of economic profits to make decisions relating to social and environmental initiatives. They may evaluate the following:

- Purchasing decisions and cost/benefit impact (E&S)
- Facility and location choices (E&S)
- Energy-efficient concepts (E)
- Manpower needs (G)

These activities can all be extended to the collection, analysis, and reporting of non-qualitative information.

Audit and assurance services. Financial statement integrity requires clear processes, procedures, and internal controls. Accountants can provide auditing and assurance on CSR or ESG reports. Systems in place and reports produced can be audited by external independent groups or individuals.

The Board's Role

The Center of Audit Quality (CAQ) found that 95 percent of S&P 500 companies had detailed ESG information publicly available, primarily outside of Securities and Exchange Commission (SEC) submission. Audit committees indicated that 66 percent of their companies issue an ESG report, and 69 percent obtain or are actively discussing obtaining third-party assurance on components of ESG or sustainability data. Recommendations by the CAQ for a company's board include the following:

- Understand the connection between ESG strategy and related goals and metrics—and how management considers any impacts it may have on the financial statements.
- Focus on internal controls/disclosure controls and procedures (DCP) for metrics publicly disclosed in a sustainability report.
- Understand how ESG risks are identified and prioritized and how materiality is defined.

- Coordinate ESG/risk oversight connections between committee members.
- Monitor assurance-related activities and oversee any third-party providing that assurance.

¶ 108 FINANCIAL REPORTING AND DCP

Companies are increasingly disclosing non-financial key performance indicators around ESG matters. Non-financial performance disclosures can provide insight into how management is navigating global trends, risks, and opportunities.

The Sustainability Accounting Standards Board (SASB) serves as a foundation for reporting the non-financial information desired by investors in addition to financial information for making investment decisions. Companies should consider what non-financial information they report and whether it meets investor needs.

In June 2020, the Investor Advisory Committee of the SEC recommended that the SEC promulgate specific guidance regarding ESG topics. Under current SEC regulations and guidance, the disclosure of ESG issues is required only if "material." In March 2021, the SEC announced the creation of a Climate and ESG Task Force in the Division of Enforcement. Information on its latest enforcement decisions related to climate and ESG is available at https://www.sec.gov/securities-topics/enforcement-task-force-focused-climate-esg-issues.

SEC Actions

The SEC has expanded and revised Regulation S-K (registration statements and annual reports) and Regulation S-X (annual audited financial statements). The changes create a new Subpart in Form 10-K related to the four pillars of governance, strategy, risk management, and metrics and targets.

The SEC voted 3–1 in March 2022 to propose rules that would address a lack of standardization in corporate reporting on climate risk. If the rules are finalized, public companies would have to report direct greenhouse gas emissions, known as Scope 1, as well as indirect pollution from purchased electricity and other forms of energy, or Scope 2. Large companies would have to give assurances about the reliability of the information.

The SEC originally set an October 2022 deadline for final rules. It found a technical glitch in its comment system, forcing it to reopen its comment period. The SEC has not provided a timeline for finishing the climate regulations, saying it needs to review thousands of comments. As of April 2023, Thomson Reuters reported: "With the reporting timeline potentially spanning from 2024 to 2027 and with a legal obligation to report, companies need to consider the full timeline and regulations with which they'll have to comply under the SEC's climate rules, once they are finalized." The proposed regulations define emissions as follows:

- Scope 1 emissions are direct emissions from sources owned or controlled by a reporting company.
- Scope 2 emissions are indirect greenhouse emissions associated with the purchase of electricity, steam, heat, and cooling.
- Scope 3 emissions are the result of activities from assets not owned or controlled by the reporting organization, but that the organization indirectly impacts in its value chain. These emissions include all sources not within an organization's scope 1 and 2 boundary.

The SEC's proposed climate disclosure rule was issued on March 21, 2022, and comments were due June 17, 2022. SEC Chairman Gary Gensler, testifying before the

U.S. House Financial Services Committee on April 18, 2022, said some 50,000 investors commented on the proposed rule with almost all in favor. Currently, under the new time frame, financial statements and disclosures under the rule would not be due until 2024. Disclosures required in registration statements (including initial public offerings) and annual reports were due at the same time as the filing.

	Financial Statements	Outside the Financial Statements
Disclosure Required	For climate-related events and transition activities: 1. Financial impact metrics 2. Expenditure metrics 3. Discussion of the impact on financial estimates and assumptions	• Greenhouse gas emission disclosures for Scopes 1, 2, and 3 • Climate governance • Climate-related risks and opportunities • Climate risk management • Climate targets and goals
Controls and Procedures	Subject to internal control over financial reporting	Subject to disclosure controls and procedures
Attestation	Part of financial statement and ICFR audit	Phase-in to reasonable assurance over Scope 1 and 2 greenhouse gas emission disclosures for large, accelerated filers and accelerated filers

¶ 109 ESG INVESTING

ESG investing is a strategy to put money to work with companies that strive to make the world a better place. It relies on independent ratings that help assess a company's behavior and policies related to ESG issues. ESG factors are part of an assessment process used to apply non-financial factors to an investor's analysis in identifying material risks and growth opportunities. ESG measures the sustainability and societal impact of an investment in a company.

Portfolio Management

The SEC expects to see investment advisers' private funds to provide accurate disclosures of ESG investing strategies and adopt and implement policies, procedures, and practices consistent with their ESG-related disclosures. The division's staff will focus on each of the following when evaluating an adviser's practices related to ESG disclosures:

- **Portfolio management.** Whether the adviser's practices are consistent with written policies, procedures, and disclosures regarding ESG investing approaches.
- **Proxy voting.** Whether the adviser's public ESG-related proxy voting claims are consistent with internal ESG disclosures and marketing materials.
- **Regulatory filings and marketing materials.** Whether the adviser's materials are consistent with actual practices and performance results, are timely updated, and contain material disclosures required.
- **Compliance programs.** Whether the adviser's written policies sufficiently address the adviser's ESG investing analysis, decision-making processes, and appropriate compliance oversight.

¶ 110 MEASURING ESG PERFORMANCE

A company's overall ESG rating is usually calculated by summing the weighted score of each unmanaged ESG risk factor. Key definitions of the main elements within ESG investing include the following:

- **ESG rating.** This rating is calculated based on a company's material exposure to company-specific and general-industry ESG risk, and how it manages those risks. The ESG rating can be calculated by summing the weighted score of all E, S, and G ratings or by focusing on individual ratings.
- **Material indicators.** Financially material ESG factors have a significant impact on a company's business model and value drivers and are a measure of performance.
- **ESG integration.** This incorporates all material ESG factors in investment analysis and decisions to determine the potential impact on the company performance.
- **Exclusions.** The use of exclusions is considered a traditional approach to considering ESG factors. This includes excluding unacceptable stocks from a portfolio, based on their ethical or environmental practices.
- **Greenwashing.** Greenwashing occurs when ESG investment products are sold as a solution to address a sustainable issue. This happens when the subsequent sustainable components' results are questionable.
- **Stewardship.** Stewardship can be thought of as the playbook (the responsible allocation, management, and oversight of capital, leading to sustainable benefits for the economy, the environment, and society).
- **Stranded assets.** These are assets that, at some point prior to the end of their economic life, become more worthless than anticipated due to the transition to a low-carbon economy (creating lower-than-expected demand or prices).

When considering ESG approaches, investors must recognize which underlying themes are producing some of the key risk factors within ESG investing. The following list highlights the more material ESG issues:

- **Climate change.** Long-term shifts in temperatures and weather patterns.
- **Biodiversity.** A measure of variation at the genetic, species, and ecosystem level.
- **Social inequality.** The condition of unequal access to the benefits of belonging to any society.
- **Supply chain management.** Companies will need to provide greater visibility into their operations related to labor practices, health and safety, and human rights.
- **Digital ethics and inclusion.** Data privacy, cybersecurity, online welfare, and ethical design of artificial intelligence (AI) and related issues. *Digital inclusion* refers to the access, skills, and benefits connected to digital technologies.
- **Corporate issuers.** ESG is not just a stock-based investment, and fixed income will grow in importance, with ESG ratings intermingling with credit ratings.

¶ 111 SUMMARY

ESG is an important movement for all companies to understand, and they should evaluate their ESG risks and opportunities. ESG issues are becoming front and central to disclosure issues; therefore, companies should proactively monitor the horizon.

STUDY QUESTIONS

4. Which of the following identifies the responsibility (related to the planet) to maintain natural resources and avoid adversely impacting the ability for future generations to meet their needs?

- **a.** Climate change
- **b.** Waste reduction
- **c.** Deforestation
- **d.** Sustainability

5. Each of the following statements is correct regarding the governance aspect of ESG, ***except?***

- **a.** The *G* in ESG refers to the governance factors of decision-making.
- **b.** S&P Global assesses companies' governance performance by assessing only two factors.
- **c.** Governance factors allow investors to screen for appropriate governance practices as they would for environmental and social factors.
- **d.** Diversity, equity, and inclusion (DEI) is another governance issue.

6. Which of the following types of performance measurements can be thought of as the playbook?

- **a.** Stewardship
- **b.** Greenwashing
- **c.** Biodiversity
- **d.** Supply chain management

MODULE 1: TOP ACCOUNTING ISSUES—CHAPTER 2: How to Account and Audit for Digital Assets

¶ 201 WELCOME

Concerns about properly accounting for and auditing digital assets have been increasing over the last decade as more and more private companies have been incorporating cryptocurrency, tokens, and other digital assets in their operations and recording them on their financial statements. This chapter will address the most frequently asked questions, specific risks, and challenges emerging in this arena.

¶ 202 LEARNING OBJECTIVES

Upon completion of this chapter, you will be able to:

- Identify how to answer frequently asked questions related to the fair presentation and disclosure of cryptocurrency and other digital assets
- Recognize common risks associated with these instruments and how to properly audit them

¶ 203 OVERVIEW

Before we begin discussing the auditing and accounting of digital assets, it is important to understand relevant key terms and concepts.

What Is Blockchain Technology?

Blockchain is a distributed, decentralized ledger where transactions are recorded and confirmed in a partial anonymous manner. Transactions, once recorded, cannot be edited, or changed. This makes blockchain immutable, at least for now. Data on the blockchain is stored in "blocks," and these blocks are cryptographically connected in a linear chain. Each block is cryptographically hashed, which makes the data secure.

Data on the blockchain is accessible to the "nodes" that are connected to the network. Each node has a copy of the entire database, and it is the blockchain technology that connects these nodes and executes the consensus protocol, based on which transactions are validated and transmitted.

What Is Cryptocurrency?

Cryptocurrency secures digital payments without the use of third-party intermediaries (i.e., banks and financial institutions). Various cryptographic techniques and encryption algorithms are used that make the transactions recorded on the blockchain secure, reliable, and tamper-resistant. Unlike fiat currencies (e.g., U.S. dollar), cryptocurrencies are generally not issued by a sovereign government or a public or private organization. This has made it a challenge to use cryptocurrency as legal tender in different international financial jurisdictions.

NOTE: Blockchain and cryptocurrency are not the same thing. Cryptocurrency is an application of blockchain software. In other words, cryptocurrency's existence is dependent on blockchain.

As of this writing, the top two most popular cryptocurrencies are Bitcoin (BTC) and Ether (ETH).

Origins of Blockchain and Cryptocurrency

Blockchain was developed in 1991 as a way to store and secure digital data. It would become more relevant after the 2008 global financial crisis, which caused many to mistrust governments and institutions. In the same year, Satoshi Nakamoto (the name taken by an anonymous entity or group of entities) published the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" to explain how Bitcoin could facilitate peer-to-peer financial transactions without the need for financial institutions and regulators.

In 2013, Vitalik Buterin built Ethereum (ETH). Ethereum added to the use cases of cryptocurrencies with the creation of "tokens" (called ERC-20 tokens) that are built on the Ethereum network. The launch of Ethereum also added many more smart contract-based use cases for cryptocurrencies.

Types and Uses of Cryptocurrency

Cryptocurrency can be classified into different forms based on how it is used:

- Cryptocurrency in its native form (e.g., BTC and ETH)
- Tokens, such as Cardano (ADA) and Algorand (ALGO), which are built on top of an existing blockchain (primarily Ethereum)
- Stable coins, such as USD Coin (USDC) and Gemini USD (GUSD), which are cryptocurrencies based on a fiat, typically at a 1:1 ratio
- Central bank digital currency (CBDC), like digital yuan, which are stable coins issued and regulated by a central government authority

According to recent statistics, the total crypto market cap was more than $2 trillion, with over 16,000 cryptocurrencies, including altcoins and stable coins.

The current Bitcoin adoption rate has been outpacing the Internet's user growth rate. Cryptocurrency adoption will likely reach 1 billion users by 2025 (two times Internet adoption). Increasing numbers of companies in the United States are accepting cryptocurrency as payments from customers, offering cryptocurrency as payment to vendors and contractors, and using it to pay their employees. Other new developments include the following:

- Banks are exploring adding offerings like cryptocurrency custody services. Major players are planning to roll out bank accounts that pay interest in Bitcoin.
- Enterprises are increasing their market share as they start accepting cryptocurrency as payment from customers, using payment processors like BitPay.
- Credit card companies have started bringing cryptocurrency into their platforms.
- Exchanges like Coinbase and Robinhood are going public.
- Cryptocurrency marketplaces have recently arisen to facilitate the buying, selling, and swapping of cryptocurrencies, including non-fungible tokens (NFTs).
- Decentralized Finance (DeFi) tools have recently arisen and can replace traditional financial systems of trading, lending, and borrowing.

Definitions

Fiat currency vs. cryptocurrency. Fiat is legal currency that is generated by a sovereign government. It is issued by a central bank and controlled by the central government. Examples of fiat include the U.S. dollar, the Euro, the British pound, etc.

Cryptocurrency is a digital asset created by blockchain software, and it is intended to be decentralized.

Tokens/altcoins. A *token* is a form of digital asset that is created using blockchain technology, for certain utilities or purposes. Tokens are typically built on top of another cryptocurrency blockchain like Ethereum. Tokens are also called *altcoins*.

- **Non-fungible tokens (NFTs):** These represent the right to ownership of a unique intangible asset on the blockchain and symbolize the digital creation of a real-world asset.
- **Governance tokens:** These are decentralized tokens that give their holders voting rights and authority over a protocol that does not have a board of directors or any central governing body.
- **Security tokens:** These tokens can be analogized to securities like stocks that operate in the traditional capital market.
- **Utility tokens:** These are tokens used for utilities like rewards and loyalty programs. They represent units of value—such as points in blockchain-based video game apps—that holders can use to purchase merchandise within an ecosystem.

Nodes. A node is a copy of the ledger, containing a complete record of all the transactions recorded on the blockchain and operated by a participant of the blockchain network.

Distributed ledger technology (DLT). DLT is a consensus of shared, digital data that is geographically spread across multiple sites, countries, or institutions. Blockchain is a type of DLT.

Hot and cold wallets. A wallet is where someone keeps their cryptocurrency, just like holding cash in a physical wallet, except that a crypto wallet is digital and can be connected to the Internet or disconnected from the Internet and created offline. A *hot wallet* is connected to the Internet; a *cold wallet* is not.

Public and private keys. Keys are long strings of random alphanumeric cryptographic code that are generated by the blockchain. *Public keys* are similar to account numbers that can be shared with others. *Private keys* are similar to email account passwords, with multilevel authentication.

Consensus mechanisms. Consensus mechanisms act as validators on the blockchain to follow certain sets of protocols to validate transactions before they get posted on the blockchain. There are two major types: Proof of Work (PoW) and Proof of Stake (PoS). Using these protocols, new transactions can be verified and added to the blockchain, and new tokens can be created. PoW was developed by Bitcoin.

Smart contracts. These are sets of codes based on business logic that are designed to execute a computer program without manual intervention once the program is running.

Public blockchain and private blockchain. A *public blockchain* (e.g., Bitcoin and Ethereum) is a distributed, open, and decentralized ledger of encrypted information, where participants can read, write, and view data. There is no single participant with complete control of the network or the data on the network. A *private blockchain* is managed by a single entity (or a group of entities), based on certain rules/consensus, and the network is closed unless someone is permitted to participate. This is a more energy-efficient network.

Gas fees. Gas is the fee that is required for an Ethereum transaction to execute successfully. Gas fees are paid in ETH.

On-chain transactions and off-chain transactions. *On-chain transactions* are blockchain-based transactions that occur when processed and successfully broadcast on the blockchain network. They incur higher costs than off-chain transactions and possible delays in processing time. *Off-chain transactions* are blockchain-based cryptocurrency transactions that occur outside of the blockchain network. These incur lower costs than on-chain transactions and offer real-time immediate settlement, with a higher level of anonymity than on-chain transactions.

¶ 204 ADVANTAGES AND DISADVANTAGES OF USING CRYPTOCURRENCY

Use of cryptocurrency presents several advantages—as well as disadvantages. Organizations must understand these in order to determine whether it makes sense to get involved in cryptocurrency.

Advantages of Using Cryptocurrency

- Increased security
- Real-time transaction updates
- Tamper-free and irreversible record history, resulting in increased authenticity of data
- Fraud protection
- Lower transaction costs
- Reduced processing time
- Smart contract benefits

Disadvantages of Using Cryptocurrency

There is an increased fraud risk over blockchain transactions due to the following:

- Weak controls over key management
- Inappropriate wallet access rights
- Lack of segregation of duties, due to inappropriate permissions to the participants in the ecosystems
- Risk of incomplete information that could lead to inaccurate and unreliable reporting
- Disintegrated systems that do not connect with blockchain without significant customization/integration
- Integrity of smart contracts and vulnerabilities in the underlying code
- Lack of standardized laws and regulations
- Lack of accounting, audit, and tax guidelines; inconsistency in valuation approaches; and lack of guidance
- Reliability of information received from third parties and their controls over reporting
- Risks due to collusion with counterparties and weak internal controls
- Difficulties with real-time reconciliation and monitoring, due to several disintegrated systems and data hosted in multiple places, including on-chain and off-chain
- Risk of unreliable, inaccurate, and incomplete data output, due to input of inaccurate data from the blockchain that can never be altered (i.e., "garbage in, garbage out")

- Difficulties in keeping up with the continuous evolution of blockchain technology and development of use cases
- General information technology and governance risks

¶ 205 HOW CRYPTOCURRENCY IS USED

Currently, cryptocurrency is used in several different ways. It is being used for banking purposes, offering financial inclusion for everyone globally who does not have access to a bank account. Remember that the premise of cryptocurrency is to facilitate peer-to-peer financial transactions without any intermediaries (i.e., banks and financial institutions). Cryptocurrency is also used for balance sheets and for payments. Uses include:

- Treasury management
- Payments for merchandise
- Cross-border payments
- Rewards and rebates
- Payroll
- Investment—buy, sell, swap, trade

Utilities of tokens is another use. As mentioned earlier, tokens are built on top of existing blockchain and are generally referred to as altcoins. Each token is designed to have a specific use case or function. Some of the use cases of tokens are as follows:

- **Tokenizing real-world assets.** Real estate, copyrights, and other real-world assets can be tokenized. Fractional ownership of assets is possible with tokenization.
- **Non-fungible tokens (NFTs).** These are crypto assets that have a unique identification code and metadata that distinguish them from each other. They represent ownership of unique items.
- **Gaming.** Tokens are used in the gaming world where they serve as a medium of exchange for goods or services, perform certain gaming actions, and more.
- **Storage.** Crypto platforms allow users to rent out unused free space on their disk and earn passive income on it.
- **Decentralized finance (DeFi).** DeFi is an emerging financial technology that is based on secure blockchain-based distributed ledgers and does not need an intermediary like a bank or a broker. DeFi tools offer buy/sell/swap on a decentralized exchange, high-yield crypto interest-bearing accounts, lending, and more.

¶ 206 CONSIDERATIONS WHEN TRANSACTING WITH CRYPTOCURRENCY

Many factors must be considered when using cryptocurrency for transactions, including accounting and financial reporting impacts; tax impacts; auditing considerations; information security risks; alternative ways of accepting and transacting cryptocurrency without any or material impact on books or taxes; information security risk considerations; and regulatory considerations.

Regulatory Concerns

In January 2023, the Office of the Comptroller of the Currency (OCC), which is charged with overseeing national banks, issued a joint statement with the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation that outlines key risks associated with crypto assets that could affect banks. The OCC

"continues to take a careful and cautious approach to banks' current and proposed crypto-asset-related activities and exposures given the significant risks highlighted by the recent failures of several large crypto-asset companies."

Infrastructure Bill Impact

The $1 trillion U.S. infrastructure bill, signed into law in 2021 by President Biden, has provisions that would allow the IRS to tax cryptocurrency trades and yield ~$2.8 billion in tax revenue.

The policy on cryptocurrency titled "Information Reporting for Brokers and Digital Assets" mandates that cryptocurrency brokers report transfers of digital assets (like a traditional broker would report the sale of a stock or bond). It requires crypto brokers to report activity to the IRS and require businesses to disclose trades of digital assets over $10,000. However, the definition of brokers is broad and unclear. It could include people who engage in any kind of cryptocurrency transaction, including miners, stakers, and software developers.

Tax Standards

Virtual currency is treated as property for U.S. federal tax purposes, and rules for property tax apply; the IRS has made few clarifications on forked assets and tax reporting. Currently, there are no plans for a specific voluntary disclosure program, but the IRS encourages all digital currency holders to self-report.

The IRS added a yes/no question to the front page of Form 1040, *U.S. Individual Income Tax Return*, asking whether filers had sold or exchanged virtual currencies. In addition, the agency has started collecting vast amounts of data on blockchain transactions, has subpoenaed crypto exchanges, and has worked on coordinating enforcement with foreign governments. The IRS is asking exchanges like Coinbase and Kraken and crypto companies like Circle to turn over customer information on cryptocurrency trades. The IRS requires reporting of any cryptocurrency transfer worth $10,000 or more.

Legalization of Cryptocurrency in El Salvador

In 2021, El Salvador became the first country to declare Bitcoin as legal tender. In September of that year, businesses in El Salvador were required to accept Bitcoin for all payments, and an official Bitcoin wallet, Chivo, was launched. New users received a sign-up bonus of $30 in Bitcoin, and 200 Chivo ATMs were deployed.

Technical challenges surrounding the legalization of Bitcoin included server capacity issues, disabled app installs, and transaction failures on launch. Money laundering issues also arose. Mass adoption is not easy to accomplish, and price volatility comes into play. There were also immediate negative implications on the country's credit rating with S&P Global. In January 2022, the International Monetary Fund (IMF) urged El Salvador to reverse its decision to use Bitcoin as legal tender, citing risks to the country's financial stability and financial integrity.

Accounting: FASB and AICPA

The American Institute of Certified Public Accountants (AICPA) has issued a guide for accounting and auditing of digital assets, but to date, the Financial Accounting Standards Board (FASB) has not issued accounting standards for cryptocurrency. Although digital assets are typically accounted for as an intangible asset, depending on the industry, they may be accounted for at fair value.

Other entities that have released regulatory updates regarding digital assets include the Financial Industry Regulatory Authority (FINRA), Commodity Futures Trad-

ing Commission (CFTC), U.S. Financial Crimes Enforcement Network (FinCEN), and the Securities and Exchange Commission (SEC). As this is an emerging area of concern, more developments are sure to come.

¶ 207 BALANCE SHEET CLASSIFICATION

Digital assets can be a very high-risk area for accountants and auditors. Accountants and auditors must understand how digital assets work, including how they are valued and maintained, to account for them appropriately. Digital assets function as a medium of exchange and have all the following characteristics:

- They're not issued by a sovereign government.
- They do not give rise to a contract between the holder and another party.
- They're not considered a "security" under the Securities Act of 1933 or the Securities Exchange Act of 1934.

These characteristics are not all-inclusive, and other facts and circumstances may need to be considered. The FASB Accounting Standards Codification (ASC) Master Glossary defines *intangible assets* as assets (not including financial assets) that lack physical substance. *Digital assets* meet the definition of intangible assets and would generally be accounted for under FASB ASC Topic 350, *Intangibles—Goodwill and Other*.

When looking at a client's financial statements that include cryptocurrencies, the first step for the accountant is to determine if the digital asset meets the definition of an asset under relevant accounting standards. Next, if the digital asset meets the definition of an asset, the accountant must determine what type of asset it is, based on the definitions of various asset classes under accounting standards. The four major classes of assets under current accounting principles generally accepted in the United States (U.S. GAAP) guidance are (1) cash and cash equivalents, (2) inventory, (3) financial instruments, and (4) intangible assets.

Cash and Cash Equivalents

Cash (and cash equivalents) is legal tender that is issued and backed by a government and accepted as a medium of exchange. Because digital assets are not legal tender issued by a government, they do not qualify under this definition.

Legal tender is specific to a jurisdiction. For example, the U.S. Code states, "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues" (Money and Finance, U.S. Code, Title 31, Section 5103, "Legal tender"). Note that the definition requires the asset to be issued by the government to qualify for this classification. Central bank digital currencies (CBDC), such as e-yuan, could qualify under this definition.

Inventory

Inventory is purchased and held in the ordinary course of business, with the intent to sell. Under U.S. GAAP, these assets need to be tangible. Inventory is recorded at the lower of cost and net realizable value (NRV). Because digital assets are not tangible, they do not qualify under this definition.

Financial Instruments

Financial instruments provide the holder with a contractual right to receive or exchange cash or a financial instrument. U.S. GAAP allows measurement of the asset at fair value and recording of changes in fair value in profit and loss.

Digital assets are not legal tender and generally do not have a contract backing any right to receive or exchange cash or a financial instrument. Therefore, they do not fall under this definition.

Depending on the contractual terms, certain cryptocurrency arrangements may be considered financial instruments. For example, cryptocurrency futures that settle in cash could be considered derivatives and thereby accounted for as financial instruments, based on this definition. Also, cryptocurrency held by organizations that fall within the scope of "investment company" status under ASC Topic 946, *Financial Services—Investment Companies*, could fall under the financial instrument definition.

Intangible Assets

Intangible assets are not physical in nature and can have definite or indefinite lives. Under U.S. GAAP, indefinite-lived intangibles are initially measured at cost and need to be tested for impairment annually or more frequently, based on triggering events. Being purely digital in nature and indefinite in life, cryptocurrencies may meet the definition of "indefinite-lived intangible assets" under U.S. GAAP.

Accounting treatment of digital assets would follow the intangible-asset guidelines under ASC Topic 350. ASC Topic 350 requires the asset to be initially recorded as an intangible asset at cost. A decline below cost in a quoted price on an exchange may be an event indicating that it is more likely than not that the digital asset is impaired.

Under ASC Topic 350, an organization should determine whether an intangible asset has a finite or indefinite life. ASC Subtopic 350-30-35-4 states that if no legal, regulatory, contractual, competitive, economic, or other factors limit the useful life of an intangible asset to the reporting entity, the useful life of the asset should be considered indefinite.

> **NOTE:** The term *indefinite* does not mean infinite or indeterminate. The useful life of an intangible asset is indefinite if that life extends beyond the foreseeable horizon—that is, there is no foreseeable limit on the period of time over which the asset is expected to contribute to the cash flows of the reporting entity.

Entities should consider the factors outlined in ASC 350-30-35-3 when determining the useful life of an intangible asset. If there is no inherent limit imposed on the useful life of the crypto asset to the entity, then the crypto asset would be classified as an indefinite-lived intangible asset. As intangible assets, these crypto assets purchased for cash would initially be measured at cost.

Accounting Impact: Acquisition of Digital Assets

Digital assets can be acquired in several ways, and each of the ways may have a different accounting treatment and may require application of other accounting guidance, such as ASC Topic 606 (*Revenue from Contracts with Customers*), ASC Topic 815 (*Derivatives and Hedging*), ASC Topic 610-20 (*Other Income—Gains and Losses from the Derecognition of Nonfinancial Assets*), and ASC Topic 845 (*Nonmonetary Transactions*).

> **EXAMPLES:** Examples of acquiring digital assets include the following:
>
> - Purchasing them directly with fiat currency from an exchange or a third-party platform that sells cryptocurrencies, such as crypto ATMs and brokers
> - Purchasing cryptocurrency with another cryptocurrency
> - Receiving cryptocurrency as payment for goods or services
> - Receiving future rights to cryptocurrency as payment for goods or services

- Receiving cryptocurrency as a donation, gift, reward, or marketing incentive
- Receiving cryptocurrency as compensation for employment
- Receiving cryptocurrency as part of a token fundraiser or crowdfunding

STUDY QUESTIONS

1. Which of the following is a copy of the ledger containing a complete record of all the transactions recorded on the blockchain and operated by a participant of the blockchain network?

a. Block
b. Token
c. Node
d. Blockchain

2. Which of the following is an advantage of using cryptocurrency?

a. Weak controls over key management
b. Real-time transaction updates
c. Inappropriate wallet access rights
d. Integrity of smart contracts and vulnerabilities in the underlying code

3. Which was the first country to adopt cryptocurrency as legal tender, starting in 2021?

a. Columbia
b. Germany
c. El Salvador
d. Canada

¶ 208 U.S. GAAP ACCOUNTING TREATMENT

When digital assets are acquired as an initial recognition, the accountant should follow the guidance under ASC Topic 350 (i.e., record the asset as an indefinite-lived intangible asset at cost, with evaluation for impairment).

Subsequent measurement assets are not subject to amortization. They are subject to annual impairment or more frequent impairment if a triggered event occurs that causes more-likely-than-not impairment of the asset. If the carrying amount of the intangible asset exceeds its fair value, an organization should recognize an impairment loss. The adjusted value becomes the new basis of the asset. If the value of the asset increases subsequently, no adjustment will be made to the cost, even if the value was recovered within the same reporting period.

If the digital asset is impaired, the organization should determine the new fair value in accordance with ASC Topic 820, *Fair Value Measurement*. For impairment assessment, the digital asset can be batched with an individual unit of another digital asset with the same carrying value and acquisition date.

U.S. GAAP Accounting Treatment Challenges

These challenges include tracking the cost basis of acquired assets and the value of acquired assets; determining what makes up an individual unit of a digital asset;

defining the triggering events for impairment, especially considering the volatility and the frequency of the reporting period for measuring impairment; and the fair value measurement of the digital asset to determine the adjusted cost basis after impairment and the value of impairment.

The receipt of the digital asset as a form of non-cash consideration under ASC Topic 606 must be considered when determining the transaction price. Management should apply all aspects of ASC Topic 606 to the transactions in the scope of that guidance (e.g., recognition, measurement, presentation, and disclosure). To determine the transaction price for the revenue contract, management would measure the digital asset at its estimated fair value at contract inception.

In ASC 606-10-32-23, any changes in the fair value of the digital asset after contract inception due to the form of the consideration would not affect the transaction price for the revenue contract. Management would apply the appropriate accounting guidance for the form of non-cash consideration to determine how any change in fair value of the digital asset should be recognized after contract inception.

An indefinite-lived intangible asset is initially carried at the value determined in accordance with ASC Topic 350 and is not subject to amortization. It should be tested for impairment annually or more frequently if events or changes in circumstances indicate it is more likely than not that the asset is impaired. If an impairment indicator exists and it is determined that the carrying amount of an intangible asset exceeds its fair value, management should recognize an impairment loss in an amount equal to that excess. After the impairment loss is recognized, the adjusted carrying amount becomes the new accounting basis of the intangible asset.

Judgment may be required to identify whether an event has occurred that would result in the need to perform an impairment assessment. When an identical digital asset is bought and sold at a price below management's current carrying value, this will often serve as an indicator that impairment is more likely than not.

Management should monitor and evaluate the quality and relevance of the available information, such as pricing information from the asset's principal (or most advantageous) market or from other digital asset exchanges or markets, to determine whether such information is indicative of a potential impairment. If management determines it is more likely than not that the indefinite-lived intangible asset is impaired, they should determine its fair value, following ASC Topic 820. If, based on its assessment, management concludes that the fair value of the digital asset is less than its carrying value, an impairment loss should be recorded.

Often, management may engage in numerous acquisitions and dispositions of digital assets during the year. They should determine the unit of account for purposes of testing the indefinite-lived intangible asset for impairment.

Management has the ability to sell or otherwise dispose of each unit (or a divisible fraction of a unit) of a digital asset separately from any other units, and they will generally reach the determination that the individual unit (or a divisible fraction of a unit) represents the unit of account for impairment testing purposes.

To perform impairment testing, management should track the carrying values of their individual digital assets (or a divisible fraction of an individual unit). When performing the impairment testing for an individual digital asset, management should compare the carrying value of that specific asset with its fair value. If management determines that an individual unit (or a divisible fraction of a unit) represents the unit of account for impairment testing purposes, it would not be appropriate to perform such comparison for a bundle of digital assets of the same type purchased at different prices.

This approach could lead to an inappropriate reduction in the amount of the impairment loss by netting (1) losses on units with carrying values above the current fair value against (2) unrealized gains on units with carrying values below the current fair value. Management could perform impairment testing for batches of digital asset units (or divisible fractions of a unit) with the same acquisition date and the same carrying value.

Management should track the cost (or subsequent carrying value) of units of digital assets they obtain at different times and use this value for each unit of digital assets upon derecognition when they sell or exchange digital assets for other goods or services.

Digital assets typically represent fungible units that can be subdivided into smaller fractional units. It may not be possible to identify which specific units of digital assets were sold or transferred in certain cases. For instance, it may be clear that the number of units of digital assets held has gone down (e.g., from 20 units to 15 units in the organization's wallet) but not whether the first, last, or some other unit purchased was the one sold. In these circumstances, management may apply the guidance by developing a reasonable and rational methodology for identifying which units of digital assets were sold and apply it consistently. For example, one reasonable and rational approach is the first in, first out (FIFO) method.

Management may transfer digital assets by exchanging them for fiat currencies, in which case, the seller should assess whether the transaction is with a customer.

- If the counterparty is a customer, management should account for the sale under ASC Topic 606 and present the sale as revenue when control of the digital assets sold has transferred.
- If the counterparty is not a customer, management should account for the sale under ASC Topic 610-20, *Other Income—Gains and Losses from the Derecognition of Nonfinancial Assets*, or ASC Topic 845, *Nonmonetary Transactions*, depending on the nature of the transfer.

In those circumstances, any gain or loss upon derecognition would typically be presented net, outside of revenue. The digital asset should be recognized on the financial statements of the organization that has control over the digital asset. Determining which organization—the depositor or the custodian—has control of the digital asset should be based on the specific facts and circumstances of the agreement between the depositor and custodian and applicable laws and regulations.

A legal assessment may be needed to evaluate certain aspects of the agreement, including legal ownership. The form of the agreement between the depositor and the custodian may vary but often will be included within the terms and conditions or initial account-opening documents provided by the custodian. Matters management may consider include the following:

- Are there legal or regulatory frameworks applicable to the custodian and the depositor (which may also depend on the jurisdiction)? If so, does the framework specify who the legal owner of the digital asset is?
- Do the terms of the arrangement between the depositor and custodian indicate whether the depositor will pass title, interest, or legal ownership of the digital asset to the custodian?
- When the depositor transfers its digital assets out of the custodian's wallet, is the custodian required to transfer the depositor's original units of the digital asset deposited with the custodian?

- Does the custodian have the right to sell, transfer, loan, encumber, or pledge the deposited digital asset for its purposes without depositor consent or notice, or both?
- Would the digital asset deposited with the custodian be isolated from the custodian's creditors in the event of bankruptcy, liquidation, or dissolution of the custodian? If not, do the depositors have a preferential claim in such circumstances?
- Can the depositor withdraw the deposited digital asset at any time and for any reason? If not, what contingencies are associated with the rights to receive the deposited digital asset? Are there technological or other factors that would prevent timely withdrawal notwithstanding contractual, legal, or regulatory rights?
- Are there side agreements affecting the rights and obligations of the depositor and the custodian?
- Are there "off-chain" transactions recorded outside of the underlying blockchain that should be considered?
- Is the digital asset held in a multi-signature wallet, and if so, what are the digital signatures that are required to execute a transaction?
- Who holds the private keys to the multi-signature wallet and how is ownership evidenced through any applicable account agreements?

If it is determined that the depositor has control over the digital asset, then the depositor should recognize the digital asset in its financial statements. If it is determined that the depositor does not have control over the digital asset—that is, the custodian has control—then the depositor should recognize a right to receive the digital asset (from the custodian) as an asset in its financial statements. The custodian should recognize the digital asset as its asset and recognize a corresponding liability to return the digital asset to the depositor in its financial statements.

The right to receive the digital asset that is recognized by the depositor and the liability to return the digital asset to the depositor that is recognized by the custodian may require further assessment for accounting purposes, including subsequent measurement considerations and assessment for embedded derivatives that may require bifurcation pursuant to ASC Topic 815.

Various Markets for Crypto Trading

The reliability and sufficiency of the information produced could vary market by market. Therefore, management should consider whether these markets provide reliable volume and level of activity information in their determination of the principal market. When identifying the principal market (or in the absence of a principal market, the most advantageous market), management is not required to undertake an exhaustive search of all possible markets for the asset, but it should consider all information that is reasonably available.

EXAMPLE: If an organization normally buys and sells crypto assets through an intermediary or a broker, it would generally identify that market as the principal market, unless it has obtained evidence (considering all information that is reasonably available) that another market (e.g., an exchange) has a greater volume and level of activity.

Accounting convention may establish a cutoff time for determining the fair value of the crypto asset. For example, it may be reasonable for management to establish an accounting convention based on prices at:

- The close of the business day of the entity
- A fixed Coordinated Universal Time (UTC)
- Other timing as deemed reasonable, such as the traditional close time based on local market jurisdictions.

Management should consider transactions that take place after the cutoff time but before the end of the reporting period. Any convention used should be reasonable and consistently applied, and changes should be made only if facts and circumstances support a change.

Stablecoins

Generally, stablecoins differ from a typical crypto asset in that they include mechanisms designed to minimize price volatility by linking their values (e.g., a "peg") to the value of a more traditional asset, such as a fiat currency or a commodity. Given the differences in the underlying rights and obligations across digital assets referred to as stablecoins, the proper accounting for an investment in a stablecoin will depend on the relevant facts and circumstances.

When evaluating the relevant facts and circumstances, key questions an entity may want to consider when determining the accounting for a holding in a stablecoin include the following:

- What is the purpose of the stablecoin?
- What are the rights and obligations of the holder?
- Is the stablecoin collateralized?
- Can the stablecoin be traded with parties other than the issuing entity?
- Who is the issuing entity (or group of entities) that is pooling resources to support the stablecoin?
- Does a legal entity that issues the stablecoin exist?
- What is the legal form of the stablecoin (e.g., debt or equity)?
- What mechanisms exist to minimize the price volatility?
- If it is redeemable, how, and how often can it be redeemed?
- If it is collateralized, how is the collateral verified and perfected? If it is collateralized, what is the level of collateral (i.e., is it partially, fully, or over-collateralized)?
- How well do the mechanisms to minimize the price volatility work?
- Do any credit or liquidity concerns exist?
- What laws and regulations apply to the stablecoin?

Because of numerous facts and circumstances that may exist, it is impossible to provide a general rule for accounting for stablecoins. Relevant U.S. GAAP should be considered. For example, the ownership of a stablecoin may provide the holder with an ownership interest in the issuing entity. Other types of stablecoins may be financial assets or financial instruments containing an embedded derivative that should be evaluated under ASC Topic 815.

¶ 209 AUDITING DIGITAL ASSETS CHALLENGES

If a public accounting firm has an insufficient understanding of the industry and environment when it accepts a client and fails to recognize and address the need for additional resources or education, it will be difficult, and might be impossible, for that firm to perform an effective audit or comply with applicable professional standards. An

auditor's ability to obtain a robust understanding of the client and its environment, including its system of internal control, is critical to an effective risk assessment and audit response.

For example, a public accounting firm may have deep experience in the financial services industry and may be presented with a client opportunity in that industry that also involves digital assets. Consideration in evaluating the client acceptance and continuance determination include a firm's (1) current industry expertise, (2) understanding of digital assets, and (3) understanding of how digital assets are being used in the specific client situation being evaluated. Knowledge of all three components is necessary for an auditor to effectively perform an engagement, and it is important to assess the ability to perform each for a well-informed client acceptance or continuance decision.

Performing audits of digital assets may require a public accounting firm to update, or include additional oversight of, its existing system of quality control. A client acceptance and continuance determination, therefore, requires an assessment both of any gaps in the skill sets of the firm's personnel and of whether the firm can satisfactorily address those gaps if it chooses to accept or continue to be engaged with the client.

Notwithstanding that the standard allows for the ability to gain the necessary knowledge for emerging issues and industries, such as digital assets, for which a firm has no previous expertise, it is important to recognize the risk of overconfidence in client acceptance and continuance decision-making and implement appropriate firm quality controls or oversight to challenge those decisions.

The digital asset environment is evolving rapidly; it is important for the firm to understand the level of effort necessary to gain the knowledge about the ecosystem (or relevant parts thereof) needed to make a reasoned client acceptance and continuance determination and competently perform the audit. Client acceptance and continuance procedures serve as a means of managing and mitigating the firm's own risks (including professional liability or external audit regulation) and informing its quality control strategy for an engagement.

Although many industries encounter change, the digital asset environment is evolving rapidly, and auditors' skill sets, and competencies may be particularly strained in this environment. In designing procedures to meet the quality control requirements of generally accepted auditing standards (U.S. GAAS), firms may encounter challenges in adapting or maintaining auditors' skill sets and competencies related to the digital asset environment in the following ways:

- Staying apprised of regulatory, industry, technological, or financial reporting developments affecting current or potential clients that may affect the risk assessment or other aspects of the audit.
- Recruiting, developing, and retaining talent in a highly competitive market, particularly those qualified in the information technology and cybersecurity aspects of the audit.
- Appropriately directing, supervising, and reviewing the work of the engagement team including staff, internal specialists, and multiple external specialists whose skill sets may not be familiar to the audit team.
- Adapting to new or different risks as the ecosystem evolves or new issues are identified.
- Updating training curricula for current and future auditors to adapt to the rapidly evolving elements of the digital asset ecosystem, new digital assets, and the surrounding business and regulatory environment.

If one or more engagements in the digital asset environment are accepted, the public accounting firm may need to consider other potential updates to the quality control system, including the following types of adjustments:

- Implement authorized lists of audit engagement partners and other individuals approved to be assigned to different roles on an audit in the digital asset environment.
- Design, implement, and commit to maintaining guidance, practice aids, tools, training, and work programs to promote consistency and quality in engagement performance, supervision, and review, particularly in the risk assessment phase and audit strategy execution on an audit in the digital asset environment.
- Establish consultation requirements for unique auditing or financial reporting issues that may be relevant in the digital asset environment.
- Update the criteria for determining which engagements require an engagement quality control review (EQCR), tailor review requirements to new or different risks, and assess the technical competence and qualifications of approved reviewers.
- Include new or high-risk engagements in the scope of pre-or post-issuance quality control monitoring procedures to evaluate engagement quality and the effectiveness of the quality control measures described herein.

Given the complexity associated with blockchain technology and digital assets, an entity's management may lack the skill sets or competencies needed to maintain the entity's books and records and secure its assets. Therefore, the assessment of whether an entity's personnel have the necessary competence and capabilities is likely an important factor related to the auditor's decision to accept or continue an audit engagement.

Even if management has integrity and a sound business strategy, if it does not have the appropriate skill sets or competencies, an audit may not be possible without management addressing the shortfalls. This may be because appropriate books and records were not maintained, processes and controls have not been implemented, or management over-relies on the auditor, thereby introducing the risk that the auditor is unable to fulfill their responsibility of providing an independent, objective opinion on the financial statements of the entity.

Further, when assessing the risks relative to the period being considered for acceptance or continuance, it is critical to understand when management obtained the necessary skill sets and competencies.

> **EXAMPLE:** If an entity recently incorporated digital assets into its business operations, it may be important for the auditor to consider management's ability to implement systems, processes, and controls over digital assets sufficient to produce high-quality financial statements free of material misstatement. Similarly, if certain actions are not taken when a transaction or control activity occurs, certain types of audit evidence may be difficult to obtain (e.g., evidence that a control related to private key management operated effectively).

Further, an entity's technical capabilities in developing digital assets technologies, although important, may not be indicative of sufficient and appropriate financial reporting capabilities or technical accounting experience. The digital asset environment presents unique considerations for auditors in the client acceptance and continuance process, which relate to both management's integrity and commitment to compliance with laws and regulations and its strategic objectives—for example, the following:

- The pseudo-anonymous nature of the digital asset transactions may present an opportunity for illegal activities such as money laundering or other illegal activities. Noncompliance with know your client (KYC) procedures, anti–money laundering (AML) procedures, and other regulations could present considerable reputation and business risks to the entity in the form of fines and penalties, both criminal and civil.
- The anonymity of participants in public blockchain transactions may make it difficult to identify transactions with related parties or "bad actors" who may have illegal or fraudulent intentions. It may also provide opportunities to engage in fraud schemes such as roundtrip transactions.
- Ease of entry to the market (i.e., anyone can market or create a digital asset) may attract those who lack integrity or a commitment to competence into the digital asset ecosystem.
- Management may not have a sufficient understanding of digital assets, the underlying technology and protocols, or the evolving regulatory environment to identify the risks related to fraud or noncompliance with laws and regulations.
- Management may assert that activities related to digital assets may not be significant or material to the financial statements; therefore, it is important for the auditor to consider noncompliance with laws and regulations (e.g., failing to meet the regulatory requirements governing the issuance of a token that might be a "security") regardless of materiality, when completing client acceptance and continuance evaluations.

If the entity stores digital assets itself, it may be important for the auditor to consider the entity's related technical capabilities, including the entity's ability to verify existence of the digital asset as well as safeguards in place to prevent digital asset loss due to fraud or error.

In most public blockchains, the underlying digital assets are bearer instruments and private keys that are lost or stolen represent irreversible, and typically uninsured, losses for the entity, with no recourse due to the decentralized nature of the blockchain. Obtaining an understanding of the entity's safeguards related to the storage and transaction initiation/authorization of digital assets, may include, but is not limited to, inquiring about the policies, processes, and controls around the following:

- The security of the physical location of the private keys;
- The processes surrounding key lifecycle management, including the key generation process (hardware, software, and algorithms associated with generation);
- The security of the entity's data centers;
- Access to private keys, including redundant private keys;
- The number of users required to process a transaction, whether through encrypting and splitting of keys or multi-signature address signing requirements; and
- Segregation of duties in the authorization of digital asset transactions.

If an entity relies on a third-party custodian to store its digital assets, the auditor considers additional risks at both the entity and the custodian. Determining the level of interaction between the entity and the custodian, including who has the ability to initiate transactions, may be critical to determining whether the preconditions for an audit are present.

EXAMPLE: Audit procedures to test digital asset ownership by obtaining signed messages may require interaction with the custodian. If so, understanding whether the custodian is willing and technically capable to assist in the audit

process helps the auditor evaluate whether the preconditions for an audit are present. As noted, professional judgment may be needed for the auditor to determine whether sufficient appropriate audit evidence can be obtained to prove ownership of the related digital asset.

As a part of the acceptance and continuance process, the auditor may seek to understand controls implemented by management to monitor service organizations. Management's controls may include performing appropriate reviews of System and Organization Controls (SOC) reports by personnel with the relevant competency and skill set and implementing complementary user entity controls. In the event SOC reports are not available, understanding alternative controls implemented by management (e.g., reconciliations of third-party data to the entity's independent books and records) will be important.

The auditor may wish to obtain the SOC report to consider whether the auditor can rely on the SOC report, as a part of the acceptance and continuance process. If the auditor is unable to determine whether the auditor can rely on the SOC report or that the scope of the report is not relevant for audit purposes, inquiring of the client about the auditor's ability to perform audit procedures at the service organization will help the auditor assess the sufficiency of audit evidence that can be obtained.

Often custodians will offer a SOC 2 report in lieu of SOC 1 reports. Although SOC 2 reports may offer greater insights on controls implemented to address trust service principles, they do not necessarily provide insights on the controls over processing of transactions for financial statement reporting.

Additionally, SOC 1 reports may not contain control objectives relating to generation, security, and monitoring of the keys used in these transactions, and the lack of this information may affect obtaining a thorough understanding of the relevant controls related to financial reporting. If a SOC report is unavailable, it is important for the auditor to consider whether additional procedures will be necessary and feasible to obtain sufficient appropriate audit evidence for reliance on information produced by the service organization.

An initial step in identifying and assessing the risk of material misstatement relating to management's rights and ownership of digital assets is understanding how the risk of loss or theft of the private keys is mitigated through storage and access controls. Obtaining an understanding of how digital assets are stored includes understanding whether the assets are held in "self-custody" or by a third party, whether the assets are stored in segregated or commingled public addresses, and to what extent private keys are stored offline (cold storage) or online (hot storage).

Entities may have different methods of storage for different digital assets, may use a combination of storage methods, and may change methods from time to time. This understanding may be obtained via observation and inquiry of appropriate personnel and inspection of internal control documentation.

When obtaining an understanding of the internal controls that the entity has implemented to safeguard digital assets, the auditor will likely determine it is important to obtain an understanding of controls that address the following:

- Hardware and software procurement and deployment (including management's due diligence over the technology)
- Initial generation of the private key
- Ongoing safeguarding of the private key
- Backups or other recovery mechanisms
- Access to perform digital asset transactions

- Segregation of incompatible duties
- IT general controls with respect to the digital wallet software
- Cybersecurity

Transacting in Digital Assets

An entity may transact in digital assets through several means and for a variety of purposes. Different means of transacting in digital assets may reflect differences in intended uses of the assets and result in different accounting considerations and risks.

Although some methods of transacting in digital assets are similar to transacting in securities and financial instruments, such as acquiring assets on an exchange or through an over-the-counter (OTC) desk, some means of transacting in digital assets, especially in the acquisition of digital assets, are unique. Methods of transacting in digital assets may include the following:

- Acquiring or transferring digital assets using a third-party exchange or OTC desk
- Acquiring digital assets as payment for selling products or services to customers
- Risk assessment and processes and controls
- Transferring digital assets for payments to vendors or employees
- Acquiring from a token issuer
- Acquiring through forks and air drops from existing digital assets owned by the entity
- Acquiring through validating activities, such as mining and staking

Digital Asset Valuation

Fair value measurements of digital assets are necessary when management measures digital assets at fair value or for an impairment analysis. The digital asset ecosystem consists of a large number of marketplaces with operations that may not have been fully developed, institutionalized, or regulated. This exposes entities to challenges in valuing digital assets.

Digital assets are commonly traded on multiple exchanges, which may result in inconsistent pricing across the various marketplaces, and not all marketplaces may be designed to prohibit self-dealing. Processes and controls should be in place to make sure that the valuation of digital assets is consistently and appropriately applied in accordance with U.S. GAAP and the entity's accounting policies.

The following are unique attributes of digital assets, which often make valuation (including the identification of impairment indicators, when applicable) more complex:

- The lack of intrinsic value of many types of digital assets
- Challenges in identifying and accessing the principal (or most advantageous) market for digital assets given that multiple marketplaces often exist globally for the same assets
- The decentralized nature of blockchain and the ability for transactions to occur between parties at any time
- Variation in levels of regulation in digital asset marketplaces

Lack of Intrinsic Value

Most traditional asset classes have clearly defined benefits or underlying cash flows that provide a basis for assessing fair value when market data is limited. For example,

financial assets often carry defined cash flow streams, which can be discounted at appropriate discount rates to estimate fair value.

Digital assets often lack even unobservable inputs from which fair values can be independently measured aside from market transactions. This lack of intrinsic value can pose challenges when estimating fair value for thinly traded digital assets. These factors likely result in higher inherent risk that these types of assets are misstated because they are not appropriately valued.

Valuation Measurement

Unlike traditional markets, the market for digital assets does not close at the end of a day, and an entity may inappropriately value its digital assets at times of the day that are not consistent across reporting periods and not in accordance with its valuation policies. This, in combination with the significant intra-day volatility of digital assets, could result in a material misstatement of valuation.

The regulatory framework of a marketplace can influence the efficacy and transparency of underlying transactions and reporting in that market. Because the same digital assets trade in disparate markets around the world with varying levels of regulation and oversight, determining the level of pricing reliability requires diligence on the part of the entity.

Not only does the pseudo-anonymity of participants in digital asset transactions create challenges for considerations related to AU-C Section 250, but it also creates unique challenges when considering the requirements of AU-C Section 550. The pseudo-anonymity creates challenges in obtaining sufficient appropriate audit evidence about whether related-party relationships and transactions have been appropriately identified, accounted for, and disclosed in the financial statements. Related-party relationships and transactions may present risk of error, illegal acts, or fraud. For example, an auditor may identify a risk of material misstatement related to the entity conducting market activities to manipulate the value of a thinly traded digital asset issued by the entity.

As another example, management may seek to materially misstate its financial position or results of operations by concealing related-party transactions or "double-counting" by asserting ownership of the same digital assets across entities (e.g., a fund complex). The challenges of meeting the requirements or objectives of U.S. GAAS, specific to the digital asset environment, may include the following:

- The pseudo-anonymity of participants in public blockchain transactions may make it difficult to identify transactions with related parties.
- Management may not have the ability or the related processes and controls to properly identify, account for, and disclose transactions with related parties.
- Sufficient appropriate evidence may not be available to demonstrate that a transaction management asserts to be arm's-length is, in fact, arm's-length. Potential risks may exist around self-dealing or "round trip transactions."
- For entities that facilitate customer transactions of digital assets (e.g., custodians and exchanges), management may not have the ability or the related processes and controls to:
  - — Distinguish between transactions on the entity's behalf and those that are on the customer's behalf;
  - — Identify employee or platform trading (e.g., conflicts of interest, self-dealing).

Procedures to obtain sufficient appropriate audit evidence about whether related-party relationships and transactions have been identified, accounted for, and disclosed in the financial statements specific to the digital asset environment include the following:

- Consider the results of client or engagement acceptance or continuance.
- Inquire with management to understand and evaluate its business purpose related to the transactions involving digital assets, including possible related-party considerations.
- Evaluate management's policies and procedures for identifying, recording, summarizing, and disclosing related-party transactions related to digital assets and perform additional procedures, including testing relevant controls, as necessary.
- Evaluate management's policies and procedures for obtaining appropriate knowledge of the parties with whom the entity is entering into digital asset transactions and perform additional procedures, including testing relevant controls, as necessary.
- Evaluate management's policies and procedures for identifying those transactions that are self-dealing or potential conflicts of interest and perform additional procedures, including testing relevant controls, as necessary.
- Examine the entity's digital asset transactions and consider whether management has appropriately identified all related-party transactions. This may include substantive procedures related to the completeness of related-party transactions identified by management. For example, obtain a listing of all entity-owned wallets and search for transactions with entity-owned wallets, obtain evidence of the counterparty to digital asset transactions by examining off-chain evidence (e.g., digital asset transaction agreements and contracts) and determine whether the counterparty is a related party.
- Test management's controls for identifying, recording, summarizing, and disclosing related-party transactions related to digital assets, if substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level.

¶ 210 EVOLVING IMPACT ON THE PUBLIC ACCOUNTING PROFESSION

In March 2023, the FASB published a proposed Accounting Standards Update (ASU), *Intangibles—Goodwill and Other—Crypto Assets (Subtopic 350-60)—Accounting for and Disclosure of Crypto Assets*, intended to improve the accounting for and disclosure of certain crypto assets. Stakeholders were encouraged to review and provide input on the proposed ASU by June 6, 2023.

"During the FASB's recent agenda consultation process, stakeholders from all professional backgrounds identified digital assets as a top priority area for the Board to address," stated FASB Chair Richard R. Jones. "We responded to that feedback with the proposed ASU, which would provide investors greater transparency into the fair value of crypto assets held by entities, as well as additional disclosures about the types of crypto assets held and changes in those holdings."

The FASB heard feedback that the accounting for crypto assets as indefinite-lived intangible assets, which is a cost-less-impairment model, does not provide investors with decision-useful information or reflect the underlying economics of those assets. The amendments in the proposed ASU would improve the accounting for certain crypto

assets by requiring an entity to measure those crypto assets at fair value each reporting period with changes in fair value recognized in net income.

The proposed amendments also would improve the information provided to investors about an entity's crypto asset holdings by requiring disclosure about significant holdings, restrictions, and changes in those holdings. The amendments in this proposed ASU would apply to all entities holding crypto assets that meet all the following criteria:

- Meet the definition of *intangible asset* as defined in the FASB Accounting Standards Codification Master Glossary
- Do not provide the asset holder with enforceable rights to, or claims on, underlying goods, services, or other assets
- Are created or reside on a distributed ledger based on blockchain technology
- Are secured through cryptography
- Are fungible
- Are not created or issued by the reporting entity or its related parties.

The public accounting profession will continue evolving as the cryptocurrency industry matures and there is more clarification from peers and standard-setting bodies on accounting treatment. Accounting and auditing professionals have an opportunity to expand their services to consulting, advisory, and project-based work, such as internal-control framework buildout, drafting internal-control narratives and flow charts, drafting technical accounting memos, and more.

Reducing the knowledge gap between accountants and IT professionals will require more collaboration and cross-functional skill sets. A deep dive into the industry and its environment will include understanding how blockchain and crypto work operationally and how entities use crypto in their business.

Accountants and auditors should work closely with external legal counsel, valuation experts, and other crypto SME to learn more about business operations and develop a control framework that will help with building accounting policies and guidelines.

¶ 211 SUMMARY

Accounting for cryptocurrencies will continue to evolve as the industry evolves and matures and there is more regulatory clarity. Peer groups have come together and are discussing practical applications to record transactions, while we wait for the accounting standard-setting bodies to formalize accounting guidance.

With the help of trusted advisors and crypto subject matter experts, there is more consistent application in financial reporting and disclosures than there was a few years ago. Entities are realizing the importance of proper accounting from day one and setting up appropriate processes, including automation.

STUDY QUESTIONS

4. Which of the following statements is correct with respect to balance sheet classification?

- **a.** The term *indefinite* does not mean infinite or indeterminate.
- **b.** Digital assets meet the definition of tangible assets.
- **c.** Legal tender is specific to an entity.
- **d.** Operating assets are purchased and held in the ordinary course of business, with the intent to sell.

5. Which of the following statements is correct with respect to U.S. GAAP accounting treatment challenges?

- **a.** After an impairment loss is recognized, the replacement cost becomes the new accounting basis of the intangible asset.
- **b.** An intangible asset with an indefinite useful life should be tested for impairment quarterly.
- **c.** To perform impairment testing, management should track the fair value of their individual digital assets.
- **d.** An indefinite-lived intangible asset is initially carried at the value determined in accordance with ASC Topic 350.

6. Which of the following statements is correct with respect to auditing digital assets?

- **a.** The digital asset environment is evolving rapidly.
- **b.** An auditor's ability to obtain a robust understanding of the client and its environment is often not critical to an effective risk assessment and audit response.
- **c.** Performing audits of digital assets does not require a firm to update, or include additional oversight of, its existing system of quality control.
- **d.** If one or more engagements in the digital asset environment are accepted, a firm must consider updates to the quality control system.

MODULE 1: TOP ACCOUNTING ISSUES—CHAPTER 3: Phishing, Vishing, and Smishing: Protecting Your Organization from Frauds

¶ 301 WELCOME

As well developed as the internal controls over information technology (IT) systems are, it is often the human element that allows criminals to commit online frauds against businesses. This chapter addresses how criminals take advantage of employees to commit data breaches or to place malware on an organization's computers. It also discusses cyber fraud awareness training and internal controls to help prevent these types of fraud.

¶ 302 LEARNING OBJECTIVES

Upon completion of this chapter, you will be able to:

- Identify phishing, vishing, and smishing
- Recognize common cyber fraud schemes
- Identify internal controls to help prevent and detect cyber frauds

¶ 303 FRAUD REVIEW

Fraud can be defined simply as making a false statement or an omission of facts that somebody else relied upon to their detriment. Fraud can be perpetrated verbally, in writing, or online. The full definition of fraud from *Black's Law Dictionary* is as follows:

> An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right. A false representation of a matter of fact, whether by words or conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury. Anything calculated to deceive, whether by a single act or combination, or by suppression of the truth, or suggestion of what is false, whether it be by direct falsehood or innuendo, by speech or silence, word of mouth, or look or gesture. A generic term, embracing all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated.[1]

Fraud Theories

The fraud triangle is a theory developed by Dr. Donald Cressey to explain why people commit fraud. The fraud triangle has three main components: (1) pressure, (2) rationalization, and (3) opportunity.

[1] Black, Henry. *Black's Law Dictionary*, Sixth Edition, West Publishing Co., St. Paul, MN, 1990.

- **Pressure** comes from the need for something, such as cash to pay bills. Dr. Cressey referred to this as an "unshakable financial need" or a need for funds that perpetrators cannot satisfy from their normal sources of money, such as their paycheck or their savings account. Unexpected expenses, car repairs, home repairs, healthcare expenses, and legal expenses—as well as the sin pressures of gambling, alcoholism, and drug addiction—can pressure people to commit fraud. Pressure can also stem from greed and spending more than one can afford.
- **Rationalization** is how individuals find ways to believe their actions are acceptable under the circumstances. Rationalization fraudsters may assert that they are only "borrowing" funds, that stealing from the government, or a company is okay because that entity can afford it, or that a computer crime is minor and does not hurt anyone.
- **Opportunity** means a criminal must have the chance to commit the fraud.

Not much can be done about outside pressures on individuals, or about somebody's ability to rationalize their behavior. After all, it is difficult, if not impossible, to change someone's thinking patterns. However, the opportunity component of the fraud triangle can be countered by developing good internal controls and cybersecurity controls over business systems.

According to the rational choice theory, developed in 1986 by Cornish and Clarke, individuals choose when and where to commit fraud. But the key part of the rational choice theory is that the higher the likelihood of the perpetrators getting caught or punished, the less likely they are to commit fraud.

We also need to consider the elements of fraud to show intent. The elements of fraud include: (1) the act, (2) concealment, and (3) conversion. *The act* consists of the actual theft or misappropriation of assets. Planning an elaborate fraud is not a crime; acting on that plan is. *Concealment* represents the perpetrator's attempts to hide the act from others. *Conversion* is the process of turning the ill-gotten gains into something the perpetrator can use. Criminals have to take what they stole, such as information from companies, governments, or IT systems, and turn it into something that has value to them, such as cash or cryptocurrencies. Internal controls help to limit the opportunity fraudsters have to commit the act or crime.

Occupational Fraud

Frauds that affect the workplace are considered occupational frauds. There are three basic types of occupational frauds: asset misappropriation, corruption, and financial statement fraud. Asset misappropriation is the theft of assets, either tangible or intangible; these can be fixed assets, inventory, or data. Corruption is the misuse of an individual's position for personal gain, and financial statement fraud is commonly referred to as "cooking the books."

According to its "Occupational Fraud 2022: A Report to the Nations," the Association of Certified Fraud Examiners (ACFE) revealed that the largest percentage of occupational fraud cases (47 percent) involved asset misappropriation. The next most prevalent category of occupational fraud was corruption (12 percent) and then financial statement fraud (1 percent of cases). Often these frauds overlap such as when a perpetrator commits financial statement fraud to cover up an asset misappropriation.

Asset misappropriations start with the basic theft of an organization's assets. Thefts of inventory, fixed assets, financial assets, data, and other intangible assets are common in today's world, with thefts of intangible assets such as crypto assets rapidly increasing in recent years. Therefore, securing both tangible and intangible assets is important for all organizations.

¶ 304 CYBER FRAUD

Cyber fraud, or crime committed via a computer or over the Internet, is on the rise. According to cyber fraud statistics from the Internet Crime Complaint Center (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf), total losses from cyber fraud were about $1.4 billion in 2017, and that amount skyrocketed to $6.9 billion in 2021 and to over $10.3 billion in 2022. The number of cyber fraud complaints rose from approximately 300,000 in 2017 to more than 800,000 in 2021. Keep in mind that these numbers reflect reported frauds only; many more frauds may be occurring that are not reported to authorities.

The IC3 study also examined specific types of frauds. For example, in 2017, approximately 25,000 victims reported losses due to phishing, vishing, and smishing. In 2021, that number rose to 323,000 victims. The numbers of data breach cases and identity theft cases have also increased significantly from 2017. Therefore, over the last five years, things have been good for cyber criminals—obviously, the COVID-19 pandemic did not slow them down.

Technology and Cyber Fraud Risk

New technology increases the risk of cyber fraud. Governments and companies are increasingly relying on technology, new technologies are being implemented, the use of electronic data storage and electronic communications is on the rise, and people generally have more access to data.

For example, many companies rapidly adopted cloud computing and online meeting services when their offices were shut down due to the COVID-19 pandemic, but many neglected to review the cybersecurity controls around these online services. Also, many companies that started using cryptocurrency did not obtain a System and Organization Controls (SOC) report on the internal controls of the crypto exchanges. Here are other examples of new technology that can pose cyber fraud risks:

- Artificial intelligence
- Smart offices
- Robotics
- Virtual reality
- Self-driving cars and trucks
- Biometrics
- Botnets of things
- Quantum computers
- Data analytics

Businesses must be aware of several risks related to cyber fraud. One is the prospect of civil litigation. For example, if a business's systems are hacked and employee and client information is stolen, those clients and employees might sue the business because it has a legal obligation to protect personal information such as names, addresses, phone numbers, Social Security numbers, and credit card numbers.

Businesses may also be subject to fines for breaches that result in personal information being compromised. In Arizona, for example, a company can be fined up to half a million dollars for failing to protect personal data.

Being hit with a data breach or other type of cyber fraud can also damage a company's reputation. People will not want to work with an organization that can't secure its own data. The organization might lose customers as well.

Sometimes government settlements come into play when a company is victim to cyber fraud. The U.S. Department of Justice or the State Attorney General's office might give the company the choice to agree to a settlement instead of being prosecuted. Most organizations will opt for the settlement, which will typically include a long-term cybersecurity audit (usually 20 years' worth), which the company must pay for.

Obviously, companies must be aware of the business disruptions that occur while they are correcting the issues from a cyberattack. And if a company is hit with ransomware, obviously ransom payments are going to cost it money, as cyber criminals will not return the stolen data for free.

Cybersecurity Risk Factors

When it comes to phishing, vishing, and smishing attacks, often a company's employees are responsible for inadvertently letting the criminals in. Many employees do not recognize the risks. They might click on links in emails, answer questions, take surveys, or go to websites that aren't cleared by the company that allow worms or other malware to be downloaded onto the organization's computer system. A lack of cybersecurity training is often to blame.

In other cases, employees override internal controls. During the COVID-19 pandemic, for example, many organizations sent their employees home with company computers and laptops and gave them high-quality virtual private network (VPN) software that encrypts and decrypts data as it passes through the Internet. Many employees took their equipment home and then turned off the VPN because it slowed down their ability to upload and download files.

Other employees plugged their company computer into their home router and modem, along with their TV, music system, gaming system, video doorbell, garage door opener, thermostat, and more. The problem is that the employee's home Internet may not be secure, putting company data at risk. Other cybersecurity risk factors related to employees include inattention, data and file sharing, and use of personal devices.

There are cybersecurity risks related to IT systems too, such as:

- Complex IT systems
- Older technology
- Bring your own device (BYOD)
- Lack of internal controls
- Ineffective cybersecurity measures
- Undertrained IT personnel
- File sharing
- Cloud computing

The Internet of Things (IoT)

The IoT includes physical objects that have sensors, software, and other technologies to connect and exchange data with other devices and systems over the Internet. According to a report by the U.S. Government Accountability Office (https://www.gao.gov/assets/gao-23-105327.pdf), "IoT devices are an outcome of combining the worlds of information technology and operational technology" and "cyber threats to critical infrastructure IoT and OT represent a significant national security challenge."

Devices with access to an IT system or to the Internet include cameras, microphones, cars, thermostats, household appliances, office equipment such as copiers, and more—and all of these can pose risks. For example, if somebody hacks a person's Alexa microphone, they can listen to all the owner's conversations. To avoid such risks, all IoT connected devices, whether at home or at the office, must be secured.

Data Breaches

A data breach involves the theft of data from computer systems belonging to companies, governmental units, and even not-for-profit organizations. Typically, large amounts of information are stolen in a short amount of time. According to statistics from the Identity Theft Resource Center (ITRC), those responsible for data breaches include the following:

- Outsiders (e.g., hackers, criminals, etc.): 62 percent of incidents
- Insiders (e.g., disgruntled employees): 11 percent of incidents
- Accidental loss: 25 percent of incidents
- State-sponsored (e.g., by countries such as China, Russia, Iran, North Korea): 2 percent of incidents

In 2022, there were more than 1,800 reported data breaches in the United States alone and over 422 million victims (http://www.idtheftcenter.org/). The ITRC also reported that the number-one way criminals breach data is through vishing, phishing, and smishing attacks, which represent 33 percent of data breach theft. The second most common method is ransomware. These two methods together account for 55 percent of data breaches.

> **NOTE:** According to the ITRC, the most frequently compromised personally identifiable information (PII) attribute in 2022 was a person's name. Social Security number and date of birth were second and third on the list, respectively.

There are multiple national laws that require organizations to keep certain information secure. Additionally, the states have a patchwork of such laws. The National Conference of State legislatures lists data breach laws by state at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Credential Stuffing

Credential stuffing is one of the ways criminals gain access to various systems. After criminals obtain user IDs and passwords through data breaches, phishing, or other means, they use software to test the acquired user IDs and passwords on various websites and computer systems. The criminal will attempt to access financial, social media, email, and other sites using the stolen information. Company and government websites are vulnerable because employees are not diligent in changing and protecting their passwords and often use the same password on multiple systems.

Organizations should monitor login failure rates as a detective control to determine if they are targets of a credential stuffing attack. Adding two-factor authentication to a website is a good preventive control to limit credential hacking. Another good internal control is requiring complex passphrases that contain an uppercase letter, a lowercase letter, a number, and a symbol; requiring users to update passwords every 90 days; and prohibiting the reuse of passwords.

Ransomware

Another risk that companies face because of phishing, vishing, and smishing attacks is ransomware. An employee clicks on a fraudulent link that allows the criminal to place

ransomware, a type of malware, on the computer. The ransomware then encrypts all the computer's files. The criminals require that the victim pay a ransom to obtain the decryption key and regain access to their files. Ransomware has been around since the late 1990s, and there are several different types. In 2021, the most common ransomware attacks came from three main programs: Revel, LockBit, and Conti.

NOTE: According to the GAO (https://www.gao.gov/assets/gao-23-106441.pdf), a ransomware attack has four stages:

1. Initial intrusion
2. Reconnaissance and lateral movement
3. Data exfiltration and encryption
4. Ransom demand

Once the deadline for the payment has passed, the criminals raise the ransom demand. Unfortunately, criminals are not always honest. When a victim makes a payment, sometimes the criminal gives them the decryption code, sometimes the criminal asks for more money, and sometimes the decryption code doesn't work, and the criminal refers the victim to a 900 number help desk where the victim pays by the minute for help decrypting their information. Governments have also been victims of ransomware.

Typical ransomware software uses RSA 2048 encryption code to encrypt files. To give an idea of how strong this code is, it is estimated it would take an average desktop computer approximately 6.4 quadrillion years to crack an RSA 2048 key.

NOTE: Ransomware does not just attack a company's servers; it can attack its email and text messaging service too.

There are many different types of ransomware. For example:

- Scareware can come in the form of pop-up ads.
- TeslaCrypt mainly affected gamers.
- Locky infects networks via malicious attachments in phishing emails.
- Wannacry targeted a Windows flaw.

There was a large increase in ransomware attacks from 2020 to 2021, and the number of attacks is expected to continue to grow. To avoid losing data due to a ransomware attack, organizations should include regular backups of their data in their internal controls.

STUDY QUESTIONS

1. Which of the following is ***not*** one of the three components of the fraud triangle?

a. Pressure
b. Opportunity
c. Motivation
d. Rationalization

2. In general, insiders are responsible for approximately what percentage of data breaches?

a. 2 percent
b. 11 percent
c. 25 percent
d. 62 percent

3. Which of the following types of ransomware is primarily contained in email?

a. Scareware

b. Locky

c. TeslaCrypt

d. Wannacry

¶ 305 PHISHING, VISHING, AND SMISHING

Phishing

According to Statista (https://www.statista.com/statistics/266161/websites-most-affected-by-phishing), the online industries most targeted by phishing attacks as of the third quarter of 2022 were, in order: financial institution, webmail, social media, logistics/shipping, retail outlet, and e-commerce/retail. Phishing statistics published by truelist.com (https://truelist.co/blog/phishing-statistics/#:~:text=Phishing%20Statistics%20%28Editor%E2%80%99s%20Choice%29%201%2082%25%20of%20people,a%20breach%20from%20compromised%20credentials.%20...%20More%20items) revealed the following:

- 82 percent of people use one password for multiple accounts. (Egress)
- Up to 98 percent of companies say they have security awareness programs in place. (Nira)
- 1.5 million new phishing websites are made monthly. (Swiss Cyber Institute)
- Stolen personal information costs $180 per record. (Egress)
- Up to 90 percent of cyberattacks are phishing attacks. (Spanning)
- It takes 250 days to discover a breach from compromised credentials. (Egress)
- Tech and pharma companies are the most vulnerable to phishing attacks. (Egress)
- The primary disguise of fraudulent emails is fake invoices. (Purplesac)

Phishing is a cybercrime in which the criminals contact the victim through email messages that appear to come from legitimate business or government sources. Social networking through phishing schemes is a common way to get around an organization's IT security. Often, the email headers are spoofed to make them look legitimate. One purpose of the phishing email is to obtain information such as names, addresses, Social Security numbers, phone numbers, dates of birth, credit card numbers, employer identification numbers (EINs), and other personal information from the victims. When the victim supplies the information, the criminals use the information to steal the victim's identity and assets. Criminals also send phishing emails containing links with the hope that the victim will click on the link and download the criminal's malware onto the victim's computer.

Criminals often try to make you think a phishing email is coming from your bank, credit card company, or other financial institution. They may indicate there is a problem with your account or that your password is expiring. Either way, they ask you to click on the link in the email and enter your user ID and password. Once they have that information, they can use your user ID and password to access your real accounts and misappropriate all your funds. Criminals also use phishing emails to try to convince you there is an issue with your social media accounts, or that your accounts need to be updated. They will stress the fact that you will lose all your posts on accounts such as

Facebook, Twitter, and LinkedIn if you don't immediately log in through the link in the email and update your account.

NOTE: According to research from KnowBe4 (https://expertinsights.com/insights/50-phishing-stats-you-should-know/), the most common subject lines in real-life phishing emails in the third quarter of 2022 were as follows:

- Equipment and Software Update
- Mail Notification: You have 5 Encrypted Messages
- Amazon: Amazon—delayed shipping
- Google: Password Expiration Notice
- Action required: Your payment was declined
- Wells Fargo: Transfer Completed
- DocuSign: Please review and sign your document
- IT: IT Satisfaction Survey
- Zoom: [manager_name] has sent you a message via Zoom Message Portal
- Microsoft: Microsoft account security code

A recent report from ESET (https://expertinsights.com/insights/50-phishing-stats-you-should-know/) found that the most common types of malicious files attached to phishing emails are Windows executables (47 percent), script files (23 percent), office documents (19 percent), PDF documents (6 percent), and shortcuts (4 percent).

Vishing

Vishing is similar to phishing except the criminals use phone calls instead of emails. For example, criminals will call a new employee or newly promoted employee, pretending to be from the employer's IT department and telling them they need to finish setting up their computer for the access they will need. The criminals tell the employee they need to remote into their computer, and then once inside the system they set up a backdoor, so they have continued access to the company's computer systems.

EXAMPLE: There was a large increase in vishing schemes in 2020 and 2021, much of it related to the fact that many employees were working from home due to COVID-19 shutdowns. An employee working from home would get a phone call from someone pretending to be from their employer's tech support department. The fraudster would tell the employee that he would be sending the employee an email containing a link to click to install company updates. When the employee clicked on the link, the criminal gained access to the company's IT system and could then install malware.

A simple internal control to avoid this this type of fraud is to train employees to request a call-back number if they receive a call from IT staff. Employees can then verify with their supervisor whether the IT call is valid.

Vishing calls are also made to alert individuals or businesses that fraud has been detected on their credit cards. The criminals use spoofed phone numbers to make it appear that the call is coming from a bank or financial institution. The criminals then ask the victim to verify information on the credit card, such as the account number, billing zip code, security code, or expiration date, in order to gain access to information that will allow them to use the credit card. Other examples of vishing phone calls include the following:

- A call informing individuals that they have won a prize but that they need to pay taxes or shipping fees to obtain it.
- A call purporting to be from the Department of Social Security alerting an individual that their Social Security number has some suspicious activity on it and that it suspended the Social Security number in response.

NOTE: Internal controls that include verification of incoming calls are important. One should never give callers access to their computer or personal information without first verifying who they are.

Smishing

Smishing is similar to phishing and vishing but is done using text messages rather than phone calls or email. Criminals try to obtain information or to get the victim to click on links so they can load malware onto the victim's devices. One smishing text claimed to be from the Federal Department of H&R Block, telling victims they needed to update their DBE Certification. It is unclear what that is, but this was obviously a fraud. Other common smishing texts spoof credit card processing platforms, banks, financial institutions, and government agencies.

¶ 306 OTHER CYBER FRAUDS

QR Code Scams

This type of fraud is accomplished when criminals place fraudulent QR codes at businesses, such as restaurants and bars, or affix fraudulent QR code stickers over the legitimate QR codes. The QR code often includes a message such as "New Menu" to entice victims to click on a malicious website designed to steal their information.

QR codes became very popular during the COVID-19 pandemic because people did not want to touch menus or papers and potentially pick up viruses. Always look for tampering or unusual placement of a QR code.

Denial of Service Attacks

Denial of service (DoS) attacks occur when criminals use infected computer networks (or botnets, which are networks of infected computers) to bring down a website or computer system by "flooding" it with large amounts of information or requests, thereby crashing the system. In many instances, the criminals follow up on the DoS attack with an attempt to hack into the system and upload malware onto the victim's computer, or steal data from the victim, while the victim is busy trying to fix the damage being done by the DoS attack.

Sockpuppets

Sockpuppets are fictitious online identities used to disguise a criminal's activity. Criminals can create a person that does not exist but has a name, an address, a Social Security number, a phone number, a resume, and a family member (think catfishing).

Pharming

Pharming is a cyber fraud in which a virus or malicious software is secretly loaded onto the victim's computer and hijacks the web browser. When the victim types in the address of a legitimate website, he or she is rerouted to a fictitious copy of the website without realizing it.

Spoofing

Spoofing is the term used to describe fraudulent email activity in which the sender's address or other parts of the email header are altered to appear as though the email originated from a different source. Spoofing is also commonly used by spammers to

hide the origin of an email for phishing, vishing, or smishing attacks. Fraudsters can also spoof websites and phone numbers. Spoofing phone numbers for vishing and smishing attacks is easy; there are even apps for that.

EXAMPLE: A common spoofing email is one sent to a company's payroll department that looks like it's from the auditor. It states that the auditor is finishing up its payroll audit and needs copies of all the employees' W-2s via email.

Cell Phone Malware and Spyware

Criminals use charging stations in public places like shopping malls or sporting events to load malware onto mobile devices that are being charged. For this reason, it is important to always use an electric plug or USB condom (a small dongle that adds a layer of protection between your device and the charging point you're attaching it to) when charging your mobile device at a public station.

Criminals also like to load spyware onto mobile devices, which allows them to listen to the owner's phone calls, read their emails, and track them with the device's GPS. Popular versions of spyware for cell phones include:

- HighsterMobile
- Spyera
- Spyrix
- FlexiSpy
- Mobile Spy
- MobiStealth
- mSpy

Keylogger, Win-Spy, Spytech Spy Agent, SpectorSoft, and 007 Spy Software are among the many other types of spyware.

STUDY QUESTIONS

4. Which of the following types of fraud is done using text messages rather than phone calls or email?

a. Phishing
b. Smishing
c. Vishing
d. Sockpuppeting

5. Which of the following describes a fraudulent email activity where the sender's address is altered to appear as though the email originated from a different source?

a. Spoofing
b. Phishing
c. Vishing
d. Smishing

¶ 307 CYBERSECURITY

When it comes to addressing cybersecurity, management is responsible for designing effective internal controls and ensuring that they are monitored and operating effectively. An entity's Board of Directors or those charged with governance have oversight

responsibilities for the entity's internal control system. The United Kingdom's National Cyber Security Centre (www.ncsc.gov.uk) promotes the following 10 Steps to Cyber Security:

1. **Set up your risk management system.** Assess the risks to your company's information and systems.
2. **Network security.** Protect your networks from attack. Defend the network perimeter, filter out unauthorized access and malicious content. Monitor and test security controls.
3. **User education and awareness.** Produce user security policies covering acceptable and secure use of your system. Include staff training. Maintain awareness of cyberattacks.
4. **Malware prevention.** Produce relevant policies and establish anti-malware defenses across your company.
5. **Removable media controls.** Have a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing into the company system.
6. **Secure configuration.** Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.
7. **Manage user privileges.** Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
8. **Incident management.** Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.
9. **Monitoring.** Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyze logs for unusual activity that could indicate an attack.
10. **Home and mobile working.** Develop a mobile working policy and train staff to follow the policy. Apply the secure baseline and build to all devices. Protect all data both in transit and at rest.

Cybersecurity Frameworks

Several organizations have released frameworks for addressing cybersecurity. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), an advisory group that helps to combat fraud, released a Framework for Internal Controls that has five components:

- Control Environment
- Control Activities
- Risk Assessment
- Information and Communication
- Monitoring

The COSO requirements for IT include the following:

- Determines Dependency between the Use of Technology in Business Processes and Technology General Controls
- Establishes Relevant Technology Infrastructure Control Activities
- Establishes Relevant Security Management Process Control Activities
- Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities

Another cybersecurity framework is the COBIT framework, which was developed by the Information Systems Audit and Control Association (ISACA) and is used in conjunction with the COSO Framework. COBIT, which stands for Control Objectives for Information Technologies, is a best practices framework that has four main domains: plan and organize, acquire and implement, deliver and support, and monitor and evaluate. The framework is often used by public companies in the United States.

ISO 27001 was created and published by the International Organization for Standardization (ISO) and is probably the most well-known standard worldwide. It is most commonly used outside the United States and by multinational companies. The standard focuses on technology and assets and concentrates on risk mitigation.

The National Institute of Standards and Technology (NIST) created the Framework for Improving Critical Infrastructure Cybersecurity that is used by government agencies and contractors and sets minimum requirements for IT security. The five components of the framework are: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover.

The Center for Internet Security (CIS) has also recommended cybersecurity controls. Its Critical Security Controls (CSCs) provide specific ways to prevent attacks and prioritize actions with high payoff results. The 20 recommended controls are outlined in the following chart:

The CIS Critical Security Controls for Effective Cyber Defense	
CSC 1	Inventory of authorized and unauthorized devices
CSC 2	Inventory of authorized and unauthorized software
CSC 3	Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
CSC 4	Continuous vulnerability assessment and remediation
CSC 5	Controlled use of administrative privileges
CSC 6	Maintenance, monitoring, and analysis of audit logs
CSC 7	Email and web browser protection
CSC 8	Malware defenses
CSC 9	Limitation and control of network ports, protocols, and services
CSC 10	Data recovery capability
CSC 11	Secure configuration for network devices such as firewalls, routers, and switches
CSC 12	Boundary defense
CSC 13	Data protection
CSC 14	Controlled access based on the need to know
CSC 15	Wireless access control
CSC 16	Account monitoring and control
CSC 17	Security skills assessment and appropriate training to fill gaps
CSC 18	Application software security
CSC 19	Incident response and management
CSC 20	Penetration tests and reaction team exercises

HITRUST is a risk and compliance framework that is primarily used in the U.S. healthcare industry. HITRUST is designed to protect personal health information (PHI) and to maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA). It defines a set of internal controls and is easily updated as regulations change. HITRUST is also easily modified for flexibility of scale (size, type, etc.).

Cybersecurity Internal Controls

A primary and very cost-effective cybersecurity internal control for businesses is limiting access to IT systems with user IDs and passphrases. As previously mentioned, businesses should require complex passphrases (see the following chart) and require employees and anyone else with access to update their passphrases every 90 days. The default local administrator passwords on all devices should be reset regularly.

When possible, businesses should use multifactor authentication or biometrics. Multifactor authentication occurs when the user inputs their user ID and passphrase and a code, usually six digits, is sent to their company cell phone. Access is denied if the code is not input within two minutes to help prevent password spraying and credential stuffing. The most common biometric authentication currently in use is facial recognition, although fingerprints, palmprints, and retina scans are also used.

Passphrase Security Chart

Length of Passphrase in Characters	Only Numbers	Mixed lowercase and uppercase alphabet characters	Mixed numbers and lowercase and uppercase alphabet characters	Mixed numbers, lowercase and uppercase alphabet characters, and special symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 seconds	10 seconds
6	Instantly	8 seconds	3 minutes	13 minutes
7	Instantly	5 minutes	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 seconds	4 days	153 days	12 years
10	40 seconds	169 days	1 year	928 years
11	6 minutes	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5b years
15	46 days	28m years	1b years	2t years
16	1 year	1b years	97b years	193t years
17	12 years	36b years	6t years	14 qd years
18	126 years	1t years	374t years	1qt years

k = thousand
m = million
b = billion
t = trillion
qd = quadrillion
qt = quintillion

Key cybersecurity internal controls also include the following:

- Router and switch controls
- Firewall (hardware and software)
- Virtual private network (VPN)
- Encryption
- Proxies
- Network intrusion prevention system (NIPS)
- Network intrusion detection system (NIDS)
- Security information and event management (SIEM)

- Spam filters
- SOC for cybersecurity (vendors and others with access)

Action Items

An organization's cybersecurity internal controls should include the following actions:

- Encrypt all files that contain important or personal information.
- Conduct a background check before hiring an employee who will have access to IT systems.
- Conduct regular training for employees on how to protect information.
- Enroll in a backup or wiping program that backs up smartphones and will allow you to remotely erase the information on a lost or stolen phone.
- Install both hardware and software firewalls.
- Encrypt all files that contain important or personal information.
- Install a good anti-virus program on computers and keep it up to date.
- Encrypt office wireless networks using WPA3.
- Do not send company information over public Wi-Fi networks.
- Do not reply to e-mails or click on links in e-mails from unknown sources.
- Use a separate computer for bank and financial transactions.
- Monitor user activity on the IT system.
- Consider getting cyber insurance.
- Have real-time monitoring of security events on the IT system.
- Update all software when vendor updates are made available.
- Use multifactor authentication or biometrics.
- Conduct regular penetration and phishing tests.

STUDY QUESTION

6. Which of the following CIS Critical Security Controls for effective cyber defense relates to having continuous vulnerability assessment and remediation?

a. CSC 1

b. CSC 2

c. CSC 3

d. CSC 4

CPE NOTE: When you have completed your study and review of chapters 1-3, which comprise Module 1, you may wish to take the Final Exam for this Module. Go to **cchcpelink.com/printcpe** to take this Final Exam online.

MODULE 2: TOP AUDITING ISSUES—CHAPTER 4: New Auditor's Reporting Standards

¶ 401 WELCOME

The Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) completed its project to update the requirements surrounding the auditor's report. With the issuance of so many new Statements on Auditing Standards (SAS) (Nos. 134 through 141), affecting the entire AU-C 700 series of AICPA *Professional Standards*, there are more requirements that audit engagement teams will need to know.

This chapter walks through the key areas of those new requirements. The auditor's report, while maintaining a good amount of the extant language, will be expanded as a result of the new standards.

¶ 402 LEARNING OBJECTIVES

Upon completion of this chapter, you will be able to:

- Identify the new requirements of the reporting under the AICPA's *Professional Standards*
- Recognize the new form and content of the updated auditor's report and when and how to modify it
- Identify the Statement on Auditing Standards (SAS) that was issued in May 2019 to improve the transparency and relevance of the communication in the auditor's report
- Identify a characteristic/change with respect to SAS No. 134
- Identify the type of audit of an employee benefit plan that used to be called a "limited scope audit" that will now be referred to as an "ERISA Section 103(a)(3)(C)" audit, subsequent to the release of SAS No. 136
- Explain the key auditing concept addressed by SAS No. 138

¶ 403 OVERVIEW

The AICPA's project to update the requirements surrounding the auditor's report resulted in the issuance of the following new reporting standards:

- SAS No. 134, *Auditor Reporting and Amendments, Including Amendments Addressing Disclosures in the Audit of Financial Statements*
- SAS No. 135, *Omnibus Statement on Auditing Standards—2019*
- SAS No. 136, *Forming an Opinion and Reporting on Financial Statements of Employee Benefit Plans Subject to ERISA*
- SAS No. 137, *The Auditor's Responsibilities Relating to Other Information Included in Annual Reports*
- SAS No. 138, *Amendments to the Description of the Concept of Materiality*
- SAS No. 139, *Amendments to AU-C Sections 800, 805, and 810 to Incorporate Auditor Reporting Changes from SAS 134*

- SAS No. 140, *Amendments to AU-C Sections 725, 730, 930, 935, and 940 to Incorporate Auditor Reporting Changes from SASs 134 and 137*
- SAS No. 141, *Amendment to the Effective Dates of SAS Nos. 134 to 140*

The changes included in each new standard will be discussed in the following sections, along with key aspects of the SAS practitioners should be aware of.

¶ 404 SAS NO. 134

SAS No. 134, *Auditor Reporting and Amendments, Including Amendments Addressing Disclosures in the Audit of Financial Statements*, was issued in May 2019 to improve the transparency and relevance of the communication in the auditor's report. Under this standard, generally accepted auditing standards (GAAS) will now be more consistent with the International Standards on Auditing (ISA).

SAS No. 134 addresses the auditor's responsibility to form an opinion on the financial statements. It also discusses the auditor's responsibilities and the form and content of the auditor's report when the auditor concludes that a modification to the auditor's opinion on the financial statements is necessary, and when additional communications are necessary in the auditor's report.

SAS No. 134 Changes

SAS No. 134 supersedes the guidance in the following sections:

- Section 700, *Forming an Opinion and Reporting on Financial Statements*
- Section 705, *Modifications to the Opinion in the Independent Auditor's Report*
- Section 706, *Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs in the Independent Auditor's Report*

SAS No. 134 adds new Section 701, *Communicating Key Audit Matters in the Independent Auditor's Report*, and also amends numerous sections of SAS No. 122 for conformity and SAS No. 132, *Going Concern*. Practitioners should pay particular attention to the following:

- The auditor's report is moved to the first section of the report.
- The Basis for the Opinion section follows the report. This section is new and more focused on the obligations relating to independence, and it clarifies that there are other ethical requirements of the audit engagement.
- The section related to auditor's responsibilities is revised, particularly as it relates to communications with those charged with governance.
  - — This section should have the heading "Auditor's Responsibilities for the Audit of the Financial Statements."
- Management and the auditor's responsibilities are evaluating and considering the conditions that give rise to the reporting entity's ability to continue as a going concern.
  - — AU-C Section 570, *The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern*, now includes a separate section when substantial doubt exists.
  - — AU-C Section 701, *Communicating Key Audit Matters in the Independent Auditor's Report*, has been added to address key audit matters (KAMs).
- KAMs are not mandated by the standard.

Management's Evaluation of Going Concern

The evaluation of going concern by management should include:

- Identification of conditions and events that could impact the entity's ability to continue as a going concern,
- How the conditions and events are addressed, and
- A conclusion by management as to the probability that the entity can mitigate and reduce to an acceptable level the effect these conditions would have on the financial conditions for a period of time.

Changes in Auditor Responsibilities

Under this SAS, the auditor's responsibilities are as follows:

- Maintain professional skepticism.
- Identify and assess the risks of material misstatement of the financial statements, whether due *to fraud or error*, and design and perform audit procedures responsive to those risks.
- Obtain an understanding of internal control.
- Evaluate the overall presentation of the financial statements.
- Conclude whether there are conditions or events, considered in the aggregate, that raise substantial doubt about the reporting entity's ability to continue as a going concern for a reasonable period of time.
- Make required communications.

Key Audit Matters

Section 701 has been added to address KAMs. In determining, communicating, and documenting KAMs, a framework has been developed. Although KAMs are not required by the standard, when the auditor is engaged by client management to communicate KAMs in the auditor's report, the framework must be utilized.

> **NOTE:** The AICPA and independent service providers typically have templates that indicate where to communicate KAMs in the proper section of the auditor's report.

KAMs are described as those matters that are the most significant in the current period audit of the financial statements. Of the matters communicated with those charged with governance, the auditor uses professional judgment to determine which of these matters are the most significant. These KAMS include:

- Areas of higher assessed risk of material misstatement, or significant risks identified in accordance with Section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*
- Significant auditor judgments relating to areas in the financial statements that involved significant management judgment, including accounting estimates that have been identified as having high estimation uncertainty
- The effect on the audit of significant events or transactions that occurred during the period

¶ 405 SAS NO. 135

SAS No. 135, *Omnibus Statement on Auditing Standards—2019*, was issued by the ASB in conjunction with SAS No. 134 to align ASB guidance more closely with guidance from the Public Company Accounting Oversight Board (PCAOB). While it amends multiple sections, the primary focus was on amending the following:

- AU-C Section 260, *The Auditor's Communication with Those Charged with Governance*
- AU-C Section 550, *Related Parties*
- AU-C Section 240, *Consideration of Fraud in a Financial Statement Audit*
- AU-C Section 260, *Communication with Those Charged with Governance*

Required Communication

The auditor's views related to significant unusual transactions could include:

- Policies and practices management used to account for these transactions
- The auditor's understanding of the business purpose
- Matters that the auditor consulted outside the engagement team that were contentious or difficult regarding the responsibility of those charged with governance to oversee the financial reporting process
- Potential effects of uncorrected misstatements on future periods

Any matters underlying those uncorrected misstatements, even if immaterial to the period under audit, could potentially cause misstatements in future periods. If management has communicated detailed information about matters that are required communication by the auditor, any omitted or inadequately described matter does not have to be communicated to those charged with governance as long as the auditor:

- Participated in management's discussion with those charged with governance, or
- Affirmatively confirmed with those charged with governance that management has adequately communicated these matters.

AU-C Section *550, Related Parties*

Changes to AU-C Section 550 address the auditor's responsibilities with regard to related-party relationships and transactions. The changes add and expand procedures in the following areas:

- Understanding of the entity and its environment
- Assessing the risks of material misstatement
- Performing audit procedures to respond to the risks
- Evaluating the audit evidence obtained
- Consideration of fraud related to risk of misstatements

AU-C Section 240, Consideration of Fraud in a Financial Statement Audit

Changes to AU-C Section 240 include redefining *significant unusual transactions* as significant transactions that are outside the normal course of business for the reporting entity or that otherwise appear to be unusual due to their timing, size, or nature.

Other Changes

Other changes in SAS No. 135 include the following:

- It adds to management's inquiries an inquiry regarding whether the reporting entity has entered into any significant unusual transaction.
- When an internal audit function exists at the reporting entity, the auditor should inquire as to whether the internal auditor is aware that the reporting entity has entered into any significant unusual transactions.
- The auditor should inquire of those charged with governance whether the reporting entity has entered into any significant unusual transactions.

- In addition, the auditor should evaluate whether the business purpose (or the lack thereof) of significant unusual transactions suggests that they may have been entered into to engage in fraudulent financial reporting or to conceal the misappropriation of assets.

¶ 406 SAS NO. 136

SAS No. 136, *Forming an Opinion and Reporting on Financial Statements of Employee Benefit Plans Subject to ERISA*, was issued to improve the communication value of the auditor's report. AU-C Section 703 includes new reporting and performance requirements that apply only to audits of financial statements for employee benefit plans that are subject to the Employee Retirement Income Security Act of 1974 **(**ERISA). The AICPA developed these requirements in consultation with the U.S. Department of Labor (DOL).

Significant changes include the following:

- The form and content of the report letter for an ERISA audit will now align with SAS No. 134 and SAS No. 135.
- Changes were made to management's election to exclude certain investment information held and certified by a qualified institution.
- A "limited scope" audit will now be referred to as an "ERISA Section 103(a)(3)(C)" audit.
- Areas of new and/or expanded requirements include:
  - — Engagement acceptance
  - — Audit risk assessment and response, which includes consideration of plan provisions
  - — Forming an opinion on ERISA financial statements
  - — Reporting on the ERISA-required supplemental schedule, including performing specific procedures
  - — Communication with those charged with governance of reportable findings that have been identified
  - — Written representations requested from management
  - — Considerations for Form 5500, *Annual Return*
  - — Communicating KAMs

Practitioners should pay particular attention to the following:

- The Scope and Nature of ERISA Section 103(a)(3)(C) Audit section is presented first.
- The Auditor's Opinion section follows the Scope and Nature section.
- The Basis for the Opinion section follows the Auditor's Opinion section.
- The Basis for the Opinion section is new and more focused on the obligations relating to independence and clarifies that there are ethical requirements of the audit engagement.
- The section related to auditor's responsibilities is revised, particularly as it relates to communications with those charged with governance. The section should have the heading "Auditor's Responsibilities for the Audit of the Financial Statements."
  - — It makes clear that the ERISA Section 103(a)(3)(C) audit does not include the certified investment information, with the exception of certain procedures.

- Improved reporting specific to going concern issue is required.
  - — AU-C Section 570 now includes a separate section when substantial doubt exists.
- ERISA required supplemental schedules are required to be recorded in an other-matter paragraph, Non-ERISA Section 103(a)(3)(C) Reports.

Engagement Acceptance

SAS No. 136 also affects engagement acceptance procedures as well as some of the requirements of AU-C Section 250, *Auditor Responsibilities*:

- Audit Risk Assessment and Response
- Prohibited Transactions
- Reportable Findings
- ERISA Section 103(a)(3)(C) Audit Procedures
- Written Representations

¶ 407 SAS NO. 137

SAS No. 137, *The Auditor's Responsibilities Relating to Other Information Included in Annual Reports*, addresses the responsibility of the auditor related to other information included in an annual report. The information can be financial or nonfinancial information.

The standard is expected to reduce diversity in practice and improve transparency related to the auditor's responsibilities for other information and documents that are within the scope of the standard. SAS No. 137 requires the auditor to read and consider consistency with the financial statements or the knowledge the auditor has obtained in the audit of the financial statements which might indicate a material misstatement of the financial statements or the other information.

NOTE: Form 5500 is not considered an annual report under SAS No. 137.

SAS No. 137 supersedes SAS No. 118, *Other Information in Documents Containing Audited Financial Statements*, as amended AU-C 720, and amends various other previously issued SASs.

Requirements of the Auditor

Under SAS No. 137, the auditor must meet several requirements.

- Obtaining the other information requires:
  - — Determining which documents comprise the annual report
  - — Obtaining management's written acknowledgement related to the documents
  - — Obtaining the entity's manner and timing of the issuances of the documents
  - — Making arrangements with management to obtain the final version of the documents in a timely manner, preferably before the date of the auditor's report
  - — Requesting that management provide written representation that a final version will be provided if after the date of the auditor's report
- Communicating with those charged with governance the following:
  - — The auditor's responsibility related to the other information
  - — The procedures performed
  - — The result of procedures performed

- Reading and considering the other information for the following:
  - — Whether a material inconsistency exits between the financial statements and the other information
  - — Comparing selected amounts or other items in the other information to the financial statements
  - — Whether a material inconsistency exists between the auditor's knowledge and the other information
  - — The existence of a material misstatement of fact or other information that is misleading

NOTE: Searching for omitted or incomplete information is not required of the auditor.

To respond when the other information appears to be misstated or is materially inconsistent, the auditor should perform procedures to determine if the other information contains a material misstatement, if the financial statements contain a material misstatement, or if the understanding of the entity and the environment needs to be updated.

Reporting

A separate section in the auditor's report titled "Other Information" should include:

- Management's responsibility for the other information.
- Identification of the other information (other information does not include the financial statement and the auditor's report).
- The auditor's opinion does not cover or express an opinion or assurance on the other information.
- The auditor's responsibility is to read the other information to determine if a material inconsistency exists concerning a material misstatement.
- Should the auditor conclude that an uncorrected material misstatement exists, that fact must be described in the auditor's report.

Required documentation includes the procedures performed, and the final version of the other information on which the procedures were performed.

¶ 408 SAS NO. 138

SAS No. 138, *Amendments to the Description of the Concept of Materiality*, was released to eliminate inconsistencies between the AICPA *Professional Standards* and the description of materiality used by the U.S. judicial system and other U.S. standard setters and regulators. The description of *materiality* has been revised as follows:

> Misstatements, including omissions, are considered to be material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

A "reasonable user" is anyone involved with the company that is likely to read the financial statements—for example, the bank, investors, lenders, an informed reader, shareholders, creditors, and so on. Therefore, auditors conducting the audit should not be thinking about what is material to the audit team, but rather what is material to those who are reading the financial statements. In forming this definition, the AICPA took into consideration what the PCAOB and the U.S. Securities and Exchange Commission (SEC) consider a reasonable investor.

¶ 409 SAS NO. 139

SAS No. 139, *Amendments to AU-C Sections 800, 805, and 810*, includes changes from SAS No. 134 in the following sections:

- Section 800, *Special Considerations—Special Purpose Frameworks*
- Section 805, *Special Considerations—Specific Elements, Accounts, or Items*
- Section 810, *Summary Financial Statements*

It also reflects guidance in new SAS Nos. 136 and 137. There are three areas of particular concern:

- Section 800 is amended to require a statement in the audit report when the financial statements are prepared on a regulatory or contractual basis of accounting, or any other basis and the use is restricted that alerts the user to the fact the financial statements may not be suitable for another purpose other than the intended purpose.
  - — In lieu of the report letter, there should be a reference to the note to the financial statements with the required information on the purpose of the financial statements.
- Section 805 adds factors to consider when reporting on a single financial statement or a specific element of a financial statement.
- Section 810 includes application paragraphs when the auditor's report includes communication about KAMs that the auditor is not required to describe the individual KAMs in the auditor's report on the summary financial statements.

¶ 410 SAS NO. 140

SAS No. 140, *Amendments to AU-C Sections 725, 730, 930, 935, and 940 to Incorporate Auditor Reporting Changes from SASs 134 and 137*, amends various sections of the AICPA's *Professional Standards*. These include:

- SAS No. 117, AU-C 935, *Compliance Audits*
- SAS No. 119, AU-C 725, *Supplementary Information in Relation to the Financial Statements as a Whole*
- SAS No. 120, AU-C 730, *Required Supplementary Information*
- SAS No. 122, *Statements on Auditing Standards: Clarification and Recodification*
- Section 920, *Letters for Underwriters and Certain Other Requesting Parties*
- Section 930, *Interim Financial Information*
- SAS No. 124, AU-C 910, *Financial Statements Prepared in Accordance with a Financial Reporting Framework Generally Accepted in Another Country*
- SAS No. 130, AU-C 940, *An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements*
- SAS No. 134, *Auditor Reporting and Amendments, Including Amendments Addressing Disclosures in the Audit of Financial Statements*
- Section 706, *Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs in the Independent Auditor's Report*
- SAS No. 136, *Forming an Opinion and Reporting on Financial Statements of Employee Benefit Plans Subject to ERISA*

¶ 411 SAS NO. 141

SAS No. 141, *Amendment to the Effective Dates of SAS Nos. 134 through 140*, delays the effective dates of SAS Nos. 134 through 140. This was done to provide relief to public accounting firms amid the challenges created by the COVID-19 pandemic. The delay is designed to ensure that CPA firms will be able to implement the new standards in the highest quality manner possible when distractions due to the pandemic subsided. SAS Nos. 134 through 140 now have effective dates for the audits of financial statements for periods ending on or after December 15, 2021.

¶ 412 CONCLUSION

To learn more about these new auditor reporting standards, auditors should visit the AICPA's website (www.aicpa.org). It has a page dedicated to the new requirements, as well as slide presentations and templates. The site is a good place to do further research on templates and on unique situations that might arise.

Reporting is key, as is ensuring that the auditor's report is tailored to each situation. Peer reviewers will be paying particular attention to whether the proper templates are used, and the auditor's report is properly customized.

STUDY QUESTIONS

1. Which of the following SASs was released to eliminate inconsistencies between the AICPA *Professional Standards* and the description of materiality used by the U.S. judicial system and other U.S. standard setters and regulators?

- **a.** SAS No. 132
- **b.** SAS No. 134
- **c.** SAS No. 137
- **d.** SAS No. 138

2. Which of the following SASs delayed the effective date of SAS Nos. 134–140?

- **a.** SAS No. 141
- **b.** SAS No. 142
- **c.** SAS No. 143
- **d.** SAS No. 144

3. SAS No. 136 relates to forming an opinion and reporting on financial statements of which of the following types of entities?

- **a.** Not-for-profit entities
- **b.** Employee benefit plans
- **c.** Private entities
- **d.** Public business entities

4. Which of the following SASs addresses the auditor's responsibilities relating to other information included in an entity's annual report?

- **a.** SAS No. 132
- **b.** SAS No. 134
- **c.** SAS No. 137
- **d.** SAS No. 138

5. Which of the following AU-C Sections was amended by SAS No. 140 and relates to required supplementary information?

a. AU-C Section 730
b. AU-C Section 910
c. AU-C Section 920
d. AU-C Section 935

6. Subsequent to the amendments from SAS No. 141, the amendments from SAS No. 138 were effective for periods ending, or for practitioners' examination or review reports dated, on or after what date?

a. December 15, 2018
b. December 15, 2019
c. December 15, 2020
d. December 15, 2021

MODULE 2: TOP AUDITING ISSUES—CHAPTER 5: How to Audit under the New Leasing Standard

¶ 501 WELCOME

This chapter is designed to provide external auditors with practical and insightful perspectives on how to audit transactions under the Financial Accounting Standards Board (FASB) Accounting Standards Codification (ASC) Topic 842, *Leases*. Topics addressed include the new accounting and financial reporting requirements and how to substantively and analytically test them in accordance with professional standards.

¶ 502 LEARNING OBJECTIVES

Upon completion of this chapter, you will be able to:

- Recognize the FASB's new leasing standard requirements
- Describe the new accounting and reporting requirements of leases
- Identify which audit procedures to perform
- Explain how to properly audit the transition requirements and initial adoption of the new leasing standard
- Identify approximately what amount of right-of-use (RoU) assets and lease payment liabilities will be added on by U.S. companies' balance sheets on account of the new lease standard
- Identify the ASU issued by the FASB on June 2, 2020, that amended the effective date of the new leasing standard
- Identify a contract, or part of a contract, that conveys the right to control the use of identified property, plant, or equipment for a period of time in exchange for consideration
- List the types of costs that are commissions or payments made to an existing tenant to terminate the lease

¶ 503 THE NEW LEASING STANDARD

Accounting Standards Update (ASU) 2016-02 introduced ASC Topic 842, which provides a lessee model that brings most leases onto the balance sheet. It aligns many of the underlying principles of the new lessor model with those in ASC Topic 606, the new revenue recognition standard (e.g., those related to evaluating when profit can be recognized). ASC Topic 842 also addresses other concerns related to the current leases model, such as eliminating the requirement in current U.S. generally accepted accounting principles (U.S. GAAP) for a company to use bright-line tests in determining lease classification.

NOTE: ASC Topic 842 is organized in the following sections:

- 10 – Overall
- 20 – Lessee
- 30 – Lessor
- 40 – Sale and Leaseback Transactions
- 50 – Leveraged Lease Arrangements

The new standard requires lessors to increase the transparency of their exposure to changes in value of their residual assets and how they manage that exposure. This new model represents a wholesale change to lease accounting. Approximately $3 trillion of RoU assets and lease payment liabilities will be added on by U.S. companies' balance sheets. Certain industries—such as retail, telecommunications, and real estate—will be severely impacted, and all other businesses that participate in leasing transactions will be affected to some degree.

Management will now face significant implementation challenges during the transition period and beyond, such as those related to:

- Applying judgment and estimating
- Managing the complexities of data collection, storage, and maintenance
- Enhancing IT systems to ensure their ability to perform the calculations necessary for compliance with reporting requirements
- Refining internal controls and other business processes related to leases
- Determining whether debt covenants are likely to be affected and, if so, working with lenders to avoid violations
- Addressing any income tax implications

Under the new standard, a lessee's financial risk metrics will change. Debt to equity will increase, and interest coverage will decrease. In addition, a lessee's financial performance metrics will change: EBITDA (earnings before interest, taxes, depreciation, and amortization) will increase, return on assets will decrease, and current ratio will decrease. Loan covenants and other long-term arrangements may be violated based on additional RoU assets and lease payment liabilities on the balance sheet.

Accounting policies and business implications will also need to be addressed. Selected considerations include:

- Budgeting and planning processes
- Lease versus buy decisions
- Internal controls over leasing transactions

Originally, FASB ASC Topic 842 was effective for private companies with annual periods beginning after December 15, 2019 (e.g., calendar periods beginning on January 1, 2020), and interim periods thereafter. Early adoption was permitted. But then the COVID-19 pandemic began.

In response, on June 3, 2020, the FASB issued ASU 2020-05, which amended the effective date of the new leasing standard to give immediate relief to private entities as a result of the widespread adverse economic effects and business disruptions caused by the pandemic. The deferral applies if those private entities have not yet issued their financial statements (or made their financial statements available for issuance) as of June 3, 2020. The effective date is now fiscal years beginning after December 15, 2021, and interim periods within fiscal years beginning after December 15, 2022.

Note that ASC Topic 842 does *not* apply to the following:

- Leases of intangible assets
- Leases to explore for or use minerals, oil, natural gas, and similar assets
- Leases of biological assets, including timber
- Leases of inventory
- Leases of assets under construction

NOTE: The new leasing standard is structured around the type of participant in the lease, as compared to the current standard, which is based on lease type.

What Is a Lease?

Under the new standard, a lease is defined as "a contract, or part of a contract, that conveys the right to control the use of identified property, plant, or equipment for a period of time in exchange for consideration." The prior definition was "an agreement conveying the right to use property, plant, or equipment (land and/or depreciable assets) usually for a stated period of time." To determine whether a contract contains a lease, the following questions should be considered:

- Is there an identified asset?
- Does the customer have the right to obtain substantially all the economic benefits from use of the asset throughout the period of time?
- Does the customer/supplier have the right to direct how and for what purpose the identified asset is used throughout the period of time?
- Does the customer have the right to operate the asset throughout the period of use without the supplier having the right to change those operating instructions?
- Did the customer design the asset (or specific aspects of the asset) in a way that predetermines how and for what purpose the asset will be used throughout the period of use?

EXAMPLE: A consumer products company, ABC, contracts with a contract manufacturer, XYZ, for a dedicated production line to manufacture one of its store-brand household products. The two-year contract specifies the type of household product, states that ABC has exclusive use of the production line, and states that XYZ must perform maintenance on the product line. ABC issues orders to XYZ about the quantity and timing of product deliveries.

Does this contract contain a lease?

Yes, because ABC has the right to use the dedicated production line for two years. The dedicated production line is an implicitly identified asset because XYZ has only one line that can fulfill the contract, and XYZ does not have the right to substitute the specified production line.

ABC has the right to control the use of the dedicated production line (identified asset) throughout the two-year period of use because:

- ABC has the right to substantially all the economic benefits from the dedicated production line over the two-year period. ABC has exclusive use of the dedicated production line and has rights to all the household products manufactured throughout the two-year period.
- ABC has the right to direct the use of the dedicated production line (identified asset). Also, ABC makes all relevant decisions regarding how and for what purpose the production line is used because it has the right to determine the quantity and timing (whether, when, and how much) of household products the production line will produce. Because XYZ is prevented from using the production line for other purposes, ABC's decision-making rights about the timing and quantity of household products produced determines when and whether the production line produces product.

Although the identified asset (dedicated production line) operation and maintenance are essential to its efficient use, XYZ's decisions here do not give it the

right to direct how and for what purpose the production line is used. As a result, XYZ does not control the production line usage. Instead, XYZ's decisions are dependent on ABC's decisions about how and for what purpose the production line is used.

¶ 504 LESSEE ACCOUNTING

Service Contracts vs. Leases

Service contracts give rise to different rights and obligations compared to those of a lease contract, which results in different accounting. In a service contract, the customer obtains economic benefit from the service only as the supplier performs the service prescribed within the contract. The vendor has a remaining obligation to perform until it has provided all of the service to the customer. The customer typically has an obligation to pay only for the services provided to date.

New Lessee Lease Classification

The lessee must now recognize both a RoU asset and an associated lease liability on the balance sheet. The FASB's view is that the lessee's right to use the underlying asset meets the definition of an asset.

The New Capital Lease/Finance Lease

A lessee is required to classify a lease as a finance lease when it meets any one of the following criteria:

- The lease transfers ownership of the underlying asset to the lessee by the end of the lease term.
- The lease grants the lessee an option to purchase the underlying asset that the lessee is reasonably certain to exercise.
- The lease term is for the major part of the remaining economic life of the underlying asset.
- The present value of the sum of the lease payments and any residual value guaranteed by the lessee that is not already reflected in the lease payments equals or exceeds substantially all of the fair value of the underlying asset.
- The underlying asset is of such a specialized nature that it is expected to have no alternative use to the lessor at the end of the lease term.

EXAMPLE: XYZ Lessee enters into a 10-year equipment lease (with no renewal options) with ABC Lessor with annual lease payments of $50,000. The economic life of the equipment is 14 years, and its fair value is $425,000. There is no purchase option available, there is no residual value guarantee made by the lessee, and the payments are due annually on January 1 of each year. The rate implicit in the lease is 5 percent. There are no other payments associated with this lease. The equipment will be returned to ABC Lessor at the end of the 10-year lease term.

Using the finance lease criteria, we can determine whether this lease is a finance or operating lease:

1. Transfer of ownership: Ownership does not transfer to the lessee.
2. Option to purchase the underlying asset: The lease does not contain a purchase option.

3. Lease term is for the major part of the remaining economic life of the underlying asset: The 10-year lease term is a major part of the economic life of the asset (10/14 = 71%).
4. Present value of the sum of the lease payments and any residual value guarantee amounts to substantially all of the fair value of the underlying asset: The present value of 10 payments of $50,000 at 5 percent is $405,391. This is approximately 95 percent of the fair value of the leased asset and is not substantially all of the fair value of the underlying asset.
5. Underlying asset is of such a specialized nature: There is no indication that this equipment is of a specialized nature.

The New Operating Lease

ASC Topic 842 states that if a lease is not a finance lease, then it is an operating lease. However, there is a short-term lease exception: a lease that at the commencement date has a lease term of 12 months or less and does not include an option to purchase the underlying asset that the lessee is reasonably certain to exercise, will not be recorded on the balance sheet. "Reasonably certain" is defined as a high degree of confidence (e.g., 85 to 90 percent) that an event will take place.

The lessee has an accounting policy option to recognize payments on a short-term lease on a straight-line basis over the lease term. If the accounting policy option is elected, short-term leases would not be reflected on the lessee's statement of financial position. A policy note disclosure is required.

Lease vs. Nonlease Components

After a lessee has made the determination that a contract contains a lease, the company is required to identify separate lease components within the contract and consider the right to use an underlying asset to be a separate lease component if both of the following conditions are met:

- The lessee can benefit from the RoU either on its own or together with other resources that are readily available to the lessee.
- The RoU is neither highly dependent on nor highly interrelated with the other right(s) to use underlying assets in the contract.

Note that not all lease contracts contain multiple lease components. When a contract does contain more than one lease component, a company is required to allocate consideration in the contract to each separate lease component and non-lease component. The following are not considered lease components and should not receive an allocation of the consideration:

- Administrative tasks to set up a contract or initiate the lease that do not transfer a good or service to the lessee, and
- Reimbursement or payment of the lessor's costs.

¶ 505 LESSEE LEASE RECOGNITION AND MANAGEMENT

Initial Measurement

The commencement date of the lease is the date on which the lessor makes an underlying asset available for use by a lessee. This date is key in determining the present value and the future minimum lease payments.

The following should be included in the lease payments relating to an underlying asset over its lease term:

- Fixed payments less any lease incentives paid or payable to the lessee
- Variable lease payments
- The exercise price of a reasonably certain option to purchase the underlying asset
- Payments for penalties for terminating the lease if the lease term reflects the lessee exercising an option to terminate the lease
- Amounts being owed under a residual value guarantee

These components should *not* be included within the lease payments:

- Certain other variable lease payments
- Guarantee by the lessee of the lessor's debt
- Amounts allocated to non-lease components

It is critical to understand the lease term. It is the sum of the non-cancellable period of the lease along with any periods covered by an option to extend the lease if the lessee is reasonably certain to exercise that option as well as any options to extend that would be controlled by a lessor.

Lease term reassessment. A significant event or change in circumstances that is within the control of the lessee directly affects whether or not the lessee is reasonably certain to exercise an option to extend or terminate the lease or to purchase the underlying asset. An event written into the contract obliges the lessee to exercise (or not to exercise) an option to extend or terminate the lease. For example:

- The lessee elects to exercise an option even though the company had previously determined that the lessee was not reasonably certain to do so.
- The lessee elects not to exercise an option even though the company had previously determined that the lessee was reasonably certain to do so.

RoU asset and lease liability. The lessee is required to measure and record both of the following:

- The lease liability at the present value of the lease payments not yet paid, discounted using the discount rate for the lease
- The RoU asset, which consists of the following:
  - — The amount of the measurement of the initial lease liability
  - — Any lease payments made to the lessor at or before the commencement date, less any lease incentives received
  - — Any initial direct costs incurred by the lessee

Discount rate. A company should use the rate implicit in the lease if it is readily determinable; if not, it should use its incremental borrowing rate. A lessee that is a private company is permitted to use a risk-free discount rate for a comparable lease term; however, the private company must make this election for all of its leases.

Initial direct costs. These are types of costs that would not have been incurred if the lease had not been obtained—for example, commissions or payments made to an existing tenant to terminate the lease. Examples of costs not identified as initial direct costs are:

- General overheads such as depreciation, occupancy, and equipment costs, and unsuccessful origination efforts and idle time
- Costs related to activities performed by the lessor for advertising, soliciting potential lessees, servicing existing leases, or other ancillary activities
- Costs related to activities that occur before the lease is obtained, such as tax or legal advice, negotiating lease terms and conditions, or evaluating a prospective lessee's financial condition

Impairment Considerations

The current lease guidance has no consideration of impairments as it relates to operating leases because there was not an asset on a lessee's balance sheet to test for impairment. Under the new guidance, the lessee will apply the ASC Topic 360 impairment guidance for its RoU assets.

After applying the impairment guidance and recording an impairment loss, the RoU asset should be measured as its carrying value less any accumulated amortization and should continue to be amortized from the date of the impairment to the earlier of its useful life or the end of the lease term.

STUDY QUESTIONS

1. Which of the following ASUs introduced a lessee model that brings most leases onto the balance sheet?

a. ASU 2016-02
b. ASU 2016-04
c. ASU 2016-05
d. ASU 2016-09

2. Which of the following types of transactions is within the scope of ASC Topic 842?

a. Leases of intangible assets
b. Leases of buildings
c. Leases of biological assets
d. Leases of inventory

3. Which of the following statements is correct regarding finance or operating leases?

a. A lessee is required to classify a lease as a finance lease when all five criteria outlined by ASC Topic 842 are met.
b. *Reasonably possible* is defined as a high degree of confidence.
c. Lessees are prohibited from recognizing payments on a short-term lease on a straight-line basis over the lease term.
d. If a lease is not a finance lease, then it's an operating lease.

¶ 506 LEASE MODIFICATIONS

Because the current guidance on lease modifications under ASC Topic 840 has generally been considered complex, ASC Topic 842 looked to simplify it. A *lease modification* is defined as "a change to the terms and conditions of a contract that results in a change in the scope of or the consideration for a lease."

In instances in which a lease modification occurs, the lessee or lessor has to determine whether the modification will be accounted for as a separate contract or as a

change to the existing contract. The lessee or lessor is required to account for a modification as a separate contract when both of the following condition exist:

- The modification grants the lessee an additional RoU not included in the original lease; and
- The lease payments increase commensurate with the stand-alone price for the additional RoU, adjusted for the circumstances of the particular contract.

If the lease modification is not accounted for as a separate contract, a company is required to reassess the classification of the lease as of the effective date of the modification based on the modified terms and conditions. Remeasurement is required under the following circumstances:

- It grants the lessee an additional RoU not included in the original contract.
- It extends or reduces the terms of an existing lease other than through the exercise of a contractual option to extend or terminate the lease.
- It changes the consideration in the contract only.
- It fully or partially terminates an existing lease.

Related-Party Leases

It is very important that the audit team distinguish related-party leases from non-related-party or third-party leases. The FASB has stated in ASC Topic 842 that the recognition and measurement for all leases should be applied by related-party lessees and lessors on the basis of legally enforceable terms and conditions of the contract, rather than at substance over form. When looking at separate financial statements of the related parties, the classification and accounting for the leases should be the same as for leases between unrelated parties.

In related-party arrangements where little documentation exists, there is nothing in writing, and the related parties frequently are under common control, the determination of whether the lease contract creates enforceable rights and obligations is, at the least, difficult. To mitigate subjectivity threats, a legal counsel assessment may be necessary.

Whether deemed subject to or exempt from ASC Topic 842, reporting entities must comply with the disclosure requirements of ASC Topic 850, *Related Party Disclosures*.

The essential practice determination that surrounds the audit engagement team in assessing whether a lease contract is enforceable is that a lease contract is no longer enforceable when both the lessee and the lessor each have the right to terminate the lease without permission from the other party with no more than an insignificant penalty. Accordingly, neither party would have enforceable rights or obligations.

Auditors should consider what impact setting a shorter lease term will have on the amortization period of leasehold improvements. The guidance indicates that leasehold improvements should be amortized over the shorter of: (1) the useful life of those leasehold improvements, and (2) the remaining lease term (unless the lease transfers ownership of the underlying asset to the lessee or the lessee is reasonably certain to exercise an option to purchase the underlying asset, in which case, the lessee should amortize the leasehold improvements to the end of their useful life).

Private companies and their external auditors will face many challenges, and many matters will be leveraged extensively on management estimates and auditors exercising professional judgment. The obstacles of common ownership with related-party leases that have no bright-line certainty are challenging with regard to: (1) whether the lease is an ASC Topic 842 lease that contains legally enforceable terms and conditions, rights, and obligations; and (2) if subject, what lease term would be applied.

¶ 507 PRESENTATION, DISCLOSURES, AND TRANSITION REQUIREMENTS

Balance Sheet

ASC Topic 842 requires that both finance lease RoU assets and operating lease RoU assets be presented separately from other assets on the statement and in the footnotes.

Income Statement

Operating leases should be included in income from continuing operations as a single lease cost, consistent with existing guidance. Components of a finance lease should be disclosed in a manner similar to how the company presents depreciation and amortization of similar assets and other interest expense.

Statement of Cash Flows

Presentation requirements for cash outflows are aligned to the presentation of expenses arising from a lease in the income statement (e.g., payments arising from operating leases should be disclosed in Cash Flows from Operating Activities).

Disclosures

Lessees are required to present both qualitative and quantitative information about their leases, the significant judgments made, and the amounts recognized in the financial statements. They should consider the level of detail necessary to satisfy disclosure objectives and appropriately aggregate and disaggregate disclosures in order to ensure the information will be useful to investors and third parties.

A lessee's qualitative disclosures include the following:

- A narrative disclosure about the options recognized and not recognized as part of its RoU assets and liabilities
- Existence of any residual value guarantees along with the related terms and conditions
- Restrictions or covenants imposed by the leases
- Significant leases that have not yet commenced to include any construction or design involvement
- Determination of the discount rate
- Election of the practical expedient for not separating lease components from non-lease components

Quantitative disclosures include the following:

- Finance lease cost, segregated between amortization of the RoU assets and interest on the lease liabilities
- Operating lease cost
- Short-term lease cost, excluding expenses relating to leases with a lease term of one month or less
- Variable lease costs
- Sub-lease income, disclosed on a gross basis, separate from finance or operating lease expense
- Net gain or loss recognized on sale and leaseback transactions

- The following amounts segregated between each type of lease:
  - — Cash paid for amounts included in the measurement of lease liabilities
  - — Supplemental non-cash information on lease liabilities arising from RoU assets
  - — Weighted average remaining lease term and discount rate
- Maturity analysis separately for both finance and operating leases

Transition Requirements

Previous operating leases should be recognized as a RoU asset at the later of the beginning of the earliest period presented in the financial statements and the commencement date of the lease. Lease liability should be measured at the present value of the sum of the following using an appropriate discount rate: (1) the remaining minimum rental payments and (2) any amounts probable of being owed by the lessee under a residual value guarantee.

Similarly, a lessee is required to measure a RoU asset as this calculated lease liability, adjusted for the following: prepaid or accrued lease payments, the remaining balance of any lease incentives received, unamortized initial direct costs, and impairment of the RoU asset, if applicable. There are two transition methods; management must choose one:

- Retrospectively to each prior reporting period presented in the financials with the cumulative effect of initially applying the new guidance at the beginning of the earliest comparative period presented.
  - — Following this method, the application date will be the later of the beginning of the earliest period presented in the financials and the commencement date of the lease. When using this approach, management applies the guidance to all periods presented in the financials.
  - — This approach will require adjustment of previously issued financials. Its reporting impact must be considered for all comparable periods presented in the financial statements issued during the year of adoption.
- Retrospectively at the beginning of the period of adoption through a cumulative effect adjustment. Following this transition method, the application date will be the beginning of the reporting period in which the reporting entity first applies ASC Topic 842.

The retrospective approach includes five optional practical expedients one may elect to apply. Practical expedients 1–3 must be elected as a package, whereas practical expedients 4 and 5 may be elected to be applied separately. The five optional practical expedients are as follows:

1. A reporting entity will not have to reassess whether any expired or existing contracts are or contain a lease.
2. A reporting entity will not have to reassess the lease classifications for any expired or existing leases—capital are finance; operating are operating.
3. A reporting entity will not have to reassess initial direct costs for any existing leases.
4. A reporting entity may also elect to use hindsight in determining the lease term when considering lease options to extend or terminate the lease and to purchase the underlying asset as well as assessing impairment of RoU assets.
5. Land easements are required to be assessed under Topic 842 to determine whether the arrangements are or contain a lease. Reporting entities can elect to not apply Topic 842 to land easements that exist or expired before the effective date of Topic 842 and that were not previously assessed under Topic 840 (ASU 2018-01).

¶ 508 SAMPLE JOURNAL ENTRIES

Sample journal entries for several different lease situations are provided in this section.

Existing Operating Lease with Practical Expedients Elected

To transition to ASC Topic 842, you would record the following journal entry at January 1, 20XX:

Account	Debit	Credit
ROU Asset	XXXX	
Accrued Rent	XXXX	
Lease Liability		XXXX
Unamortized IDCs		XXXX

You would record the following journal entry at December 31, 20XX (with similar entries throughout the term of the lease):

Account	Debit	Credit
Lease Liability	XXXX	
Lease Expense	XXXX	
ROU Asset		XXXX
Cash		XXXX

Existing Capital Lease with Practical Expedients Elected

To transition to ASC Topic 842, you would record the following journal entry at January 1, 20XX, in order to add the unamortized IDCs to the initial ROU asset:

Account	Debit	Credit
ROU Asset	XXXX	
Capital Lease Asset		XXXX
Unamortized IDCs		XXXX

You would record the following journal entry at December 31, 20XX (with similar entries throughout the term of the lease):

Account	Debit	Credit
Lease Liability	XXXX	
Amortization Expense	XXXX	
Interest Expense	XXXX	
ROU Asset		XXXX
Cash		XXXX

At the end of the lease term, you would record the following journal entries:

Account	Debit	Credit
Lease Liability	XXXX	
Amortization Expense	XXXX	
Interest Expense	XXXX	
ROU Asset		XXXX
Cash		XXXX
Lease Liability	XXXX	
ROU Asset		XXXX
Cash		XXXX

Initial Measurement of ROU Asset and Lease Liability under ASC Topic 842

You would record the following journal entry at January 1, 20XX:

Account	Debit	Credit
ROU Asset	XXXX	
Lease Liability		XXXX
Cash		XXXX

You would record the following journal entry at December 31, 20XX (with similar entries throughout the term of the lease):

Account	Debit	Credit
Lease Liability	XXXX	
Lease Expense	XXXX	
ROU Asset		XXXX
Cash		XXXX

Accounting for a Finance Lease under ASC Topic 842

You would record the following journal entry at January 1, 20XX:

Account	Debit	Credit
ROU Asset	XXXX	
Lease Liability		XXXX
Cash		XXXX

You would record the following journal entry at December 31, 20XX (with similar entries throughout the term of the lease):

Account	Debit	Credit
Lease Liability	XXXX	
Amortization Expense	XXXX	
Interest Expense	XXXX	
ROU Asset		XXXX
Cash		XXXX

NOTE: Lessons learned from both public business entities and privately held companies that have adopted the new leasing standard include the following:

- Leases are not that easy to find.
- Required lease information can be a real challenge to abstract, migrate, and maintain.
- Systems and processes may require more attention than expected or needed.
- Calculation of incremental borrow rate is difficult.
- Implement ASC Topic 842 as soon as possible.

¶ 509 INQUIRY WITH MANAGEMENT REGARDING TRANSITION

The extent of the engagement team's inquiry and discussion with management concerning the transition to ASC Topic 842 will depend on the nature and volume of the client's contracts related to property, including service agreements. The engagement team will need to discuss with management the accounting requirements of the new guidance to

assess whether the client is adequately planning for the transition, including the use of the practical expedients and accounting policy elections that are available. The team may also want to discuss the associated business and tax implications.

A threshold issue is the capability of the client's personnel to plan and execute the transition to ASC Topic 842.

- Is it realistic to expect someone among accounting personnel to function as an in-house lease specialist?
- Can that person, or another member of management, head the effort to identify all agreements that are or contain leases, and collect the information that will be needed for implementation of the new requirements?
- Will it be necessary to engage an outside expert or otherwise outsource some of the necessary activities?

Existing arrangements should be surveyed to identify leases or embedded leases and collect the data that will be needed on each one, including counterparty information, lease term and renewal and termination options, payment terms, and details of the property explicit or implicit in the agreement.

Management will also need to make decisions about establishing a central depository for the data and extent to which new technology may be necessary to properly accumulate and analyze the information.

The engagement team will need to discuss with management the implications of the available elections possible in the transition to the new guidance. For example, electing to not separate lease and non-lease components or use the risk-free rate as the discount rate will make the transition easier and less time-consuming but will result in larger asset and liability balances.

In addition, using hindsight to determine lease terms and impairment avoids estimates and judgments, but must be applied consistently to all expired or existing leases and may interfere with the election for short-term leases. If one or more 12-month leases had renewal options that were not reasonably certain to be exercised at inception, but were in fact exercised, they could not be treated as short-term leases.

The engagement team should discuss business and tax implications, as well as the effects on loan covenants, buy-or-lease decisions, and structuring of lease contracts that may point toward revising agreements.

Because the prior leasing guidance resulted in operating leases being off balance sheet, the change to all leases being on the balance sheet may result in loan covenant violations, may change the economics of deciding to lease rather than buy, or may change previous decisions to structure an agreement to obtain classification as an operating lease.

ASC Topic 842 does not change lease characterization for federal income tax purposes, but may result in recording new, or adjusting existing, deferred tax assets and deferred tax liabilities. Common book–tax differences are a lessee expensing rent on a straight-line basis for book purposes, but expensing rent payments as made for tax purposes; or depreciating a RoU asset on a straight-line basis for book purposes, but differently for tax purposes.

¶ 510 AUDITING UNDER THE NEW LEASING STANDARD

When auditing under ASC Topic 842, auditors should take the following actions:

- Obtain from the client an analysis of lease contracts separated by class of asset, including those that existed at the end of the prior year and any new lease contracts, showing the balance of RoU lease assets and lease liabilities at the beginning and end of the period, and the related amortization and interest expense.
- Test the clerical accuracy of the analysis.
- Trace the opening balances to the adjusted prior-year working trial balance and the ending balances to the current-year working trial balance.
- Review any reconciliation to the general ledger and investigate any unusual reconciling items.
- Compare and document (including your expectations) balances in the lease liability accounts and related interest expense with those of the preceding years or other expectations.
- Compare and document (including your expectations) balances in the RoU asset accounts and related amortization with those of the preceding years or other expectations.
- Investigate any unexpected results (ratios or variations different from what would be expected), considering known changes in client operations.
- For any leases that were not tested in a prior audit or were significantly modified in the current period, the auditor should perform the following procedures:
  - — Obtain and review lease contracts and other applicable documents and review abstracts or copies of significant lease contracts analyzed in prior years.
  - — Based on your knowledge of the client's business and industry, inquire whether outsourcing, service, supply, or other similar contracts give the client the right to control an identified asset (i.e., embedded lease).
  - — Determine that the contracts contain a lease as defined in and that the client has identified the separate lease components (or multiple components) and non-lease components, if any, within each contract and has allocated the consideration in the contracts to each separate lease and non-lease component of the contract.
  - — Consider whether to confirm significant lease obligations and related lease provisions.
- Based on the terms of the contracts, determine that leases are appropriately classified as either finance or operating leases and that initial measurement of the RoU asset and lease liability are in accordance with ASC Topic 842.
- Inquire about whether any major sales of fixed assets were sale-leaseback transactions. If so, determine the propriety of accounting for those transactions.
- Determine that significant related-party leases are classified and accounted for on the basis of the legally enforceable terms and conditions of the lease in the same manner as leases between unrelated parties.
- Evaluate whether (1) any modifications to the lease during the period are appropriately accounted for as either changes to an existing lease contract or as a separate lease contract and (2) any other circumstances have occurred that require the lessee to remeasure the lease liability.

- Considering information obtained in performing other procedures and knowledge of client operations and business conditions, evaluate whether the remaining useful lives of RoU assets are reasonable and the net carrying values of RoU assets are recoverable in the ordinary course of business.
- Considering the procedures previously performed related to RoU assets and lease liabilities, including lease modifications, if any, perform the following procedures:
  - — Evaluate the reasonableness of interest expense for the period and any related accrued amount at the balance sheet date.
  - — Test the adequacy of amortization for the period and related accumulated amortization.
- Evaluate whether the balance sheet presentation of RoU assets and lease liabilities is consistent with the requirements and whether expenses related to leased assets are appropriately presented in the statement of comprehensive income.
- Summarize the financial statement disclosures in the workpapers for both finance and operating leases.

STUDY QUESTIONS

4. Which of the following identifies the date on which the lessor makes an underlying asset available for use by a lessee?

a. Transfer date

b. Commencement date

c. Activity date

d. Transaction date

5. Which of the following statements is correct regarding presentation, disclosure, and transition to the new lease standard?

a. Lessees are required to present both qualitative and quantitative information about their leases.

b. Both finance lease RoU assets and operating lease RoU assets should be presented together with other assets on the statement and in the footnotes.

c. Operating leases should be excluded from income from continuing operations as a single lease cost.

d. Payments arising from operating leases should be disclosed in cash flows from investing activities.

6. Each of the following identifies an auditing procedure to be performed regarding the new lease standard, ***except?***

a. Obtain from the client an analysis of lease contracts separated by class of asset.

b. Trace the opening balances to the adjusted prior-year working trial balance and the ending balances to the current-year working trial balance.

c. Determine that leases are appropriately classified as either finance or operating leases.

d. Assess the reasonableness of the valuation of RoU assets recorded for short-term leases.

MODULE 2: TOP AUDITING ISSUES—
CHAPTER 6: The Future of Internal Audit

¶ 601 WELCOME

This chapter discusses what the future holds for internal auditors. Topics covered include how to address challenges and emerging risks, and the importance of staying relevant, being proactive, upgrading skills, and understanding the role of technology. It also briefly discusses the Institute of Internal Auditors proposed *Global Internal Audit Standards* that will replace the International Professional Practices Framework for internal auditors.

¶ 602 LEARNING OBJECTIVES

Upon completion of this chapter, you will be able to:

- Explain the context of the proposed *Global Internal Audit Standards*
- Identify the challenges for auditors to stay relevant in a changing business environment
- Identify challenges to the traditional audit process
- Identify top emerging risks for internal audit
- Explain how to evaluate the impact of the changing environment (due to COVID-19) on the work plan of internal audit
- Identify and examine actions internal audit can take to address challenges
- Recognize the importance of upgrading the skills and exposure of the internal audit team
- Recognize the role of technology in assuring a smooth transition to value-added auditing

¶ 603 INTRODUCTION

The COVID-19 pandemic impacted all professions, and internal audit is no exception. As if communicating and conducting an internal audit on-site are not challenging enough, auditors are facing the challenges of remote work and a rapidly changing risk and technology environment. With the onset of the pandemic in 2020, internal audit departments saw their audit plans changing and adapting. In many cases, internal resources were reallocated to operational areas. In other instances, plans were deferred or dramatically altered. In addition to these challenges, internal audit faced challenges with:

- Emerging business risks and technologies
- Audit plan priorities
- Staff skills
- Department resources

Organizations, their environments, and their ways of working have evolved rapidly and in ways that had not been previously envisioned. This includes everything from reallocation of work responsibilities to being expected to conduct internal audits remotely. Internal audit must look within to determine how to stay relevant and add value

in this changing environment. It is important that internal auditors be proactive and prepared, while remaining pragmatic, as the situation continues to evolve.

¶ 604 STANDARDS UPDATE

The current *Standards* promulgated by the Institute of Internal Auditors (IIA) are principle-focused and provide a framework for performing internal auditing. They are IIA mandatory requirements consisting of statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance, interpretations clarifying terms and concepts, and glossary terms.

In 2020, the IIA undertook an extensive review to update the *IIA Standards*. The purpose was to:

- Simplify the structure of the *International Professional Practices Framework (IPPF)*, which is the conceptual framework that organizes the IIA's authoritative guidance;
- Clarify and align all elements of the *Standards*; and
- Ensure the *Standards* are timely, practical, and applicable and address emerging topics.

The IIA Standards Board solicited input on the proposed *Standards* from 3,600 internal audit practitioners from 159 countries via a 2021 survey. The public comment period on the proposed *Standards* ran from March 1 through May 30, 2023. Representatives from 115 IIA Global Affiliates provided input regarding the proposed changes via webinars, surveys, in-person and virtual Q&A sessions, and two Global Assembly meetings. More than 70 stakeholder organizations, including regulators, standard-setting bodies, and thousands of practitioners, participated.

At the time of this writing, the official release of the finalized update is scheduled for the end of 2023. The following is a preview of some of the main concepts of the proposed *Standards*.

> **NOTE:** The IIA's proposed *Global Internal Audit Standards* will not be divided into "Attribute" and "Performance" categories and will not contain "Interpretations" as a separate section of the *Standards*. These attributes have been incorporated into the main body of the proposed *Standards*. Also, the numbering system and order of the *Standards* has changed completely.

The new name for the *Standards* is *Global Internal Audit Standards*, and it has a new structure. Content from six elements of the current IPPF (Mission, Definition, Code of Ethics, Core Principles, Standards, and Implementation Guides) are incorporated into the following five domains in the new *Standards*:

- Purpose of Internal Auditing contains elements of the current definition/mission of Internal Audit.
- Ethics and Professionalism incorporates and builds upon the current Code of Ethics.
- Governing the Internal Audit Function focuses on the relationship between the board and the Chief Audit Executive (CAE).
- Managing the Internal Audit Function focuses on requirements for the CAE to effectively manage internal audit.
- Performing Internal Audit Services focuses on performing assurance and advisory engagements.

There are new sections in each *Standard*. Each *Standard* will include sections describing the following:

- The requirements of the Standard
- Considerations for implementing the requirements and common/preferred practices for implementation
- Considerations for providing evidence of conformance and examples of recommended ways to demonstrate the requirements have been implemented

The first domain in the proposed *Standards*, Purpose of Internal Auditing, incorporates the mission of Internal Audit and the definition of Internal Audit from the current *Standards*, and, for the first time, addresses how internal audit helps organizations serve the public interest.

The Code of Ethics has been incorporated into the Ethics and Professionalism domain and contains standards for due professional care, professional skepticism, and minimum requirements for continuing professional development for all internal auditors.

The new Governing the Internal Audit Function domain clarifies the definition and use of the term *board* and the board's role in governing the internal audit function.

Board responsibilities related to the internal audit function (which were implied in the existing *Standards*) are stated more directly. These include responsibilities related to oversight of the performance of the CAE and the internal audit function, including external quality assessments.

New and changed requirements for the quality assurance and improvement program include a description of the requirements for board oversight of the program and the requirement for at least one reviewer in an external quality review to be a Certified Internal Auditor (CIA).

Special attention is paid to the public sector in the proposed *Standards*. In addition, a new Considerations for Implementation section specifically addresses information to assist internal auditors in the public sector.

The *Global Internal Audit Standards* outline a rigorous standard-setting process and provide an increased focus on stakeholders and the public interest. The proposed *Standards* include new terms and a revised and expanded Glossary. For clarity, the proposed *Standards* introduce and define terms such as:

- Criteria/condition
- Finding
- Inherent risk/residual risk
- Public sector
- Risk tolerance
- Root cause

The IIA provides a detailed mapping of the current *Standards* to the proposed *Global Internal Audit Standards* at https://www.theiia.org/globalassets/site/standards/ippf/standards-mapping.pdf.

¶ 605 CHALLENGES WITH THE NEW STANDARDS

The proposed revisions to the *Standards* were released in March 2023. Many opinions and some concerns about the changes have been expressed, including those related to the following:

- Use of the word *must* throughout the proposal
- The proposal relating to the board of directors' responsibilities and internal audit

- Internal auditors' need to adapt to new technologies, collaborate with other functions, and be more strategic in their approach in the future
- Mandated ratings or rankings for internal audit engagement findings and a rating for the aggregated engagement results
- Requirements for obtaining and maintaining the Certified Internal Auditor Certification through the IIA

In relationship to the concept of assigning ratings, the IIA had left the decision to the professional judgment of the internal audit team. However, if the proposed *Standards* are adopted, discretion will be a thing of the past. According to Proposed *Standard* 14.3, Evaluation of Findings—Requirements, "Internal audit must provide a rating, or other indication of priority for each engagement finding, based on significance of finding, using methodologies established by the CAE . . . Where appropriate, the internal auditors' opinion should be provided."

Proposed Standard 14.5, Developing Engagement Conclusions—Requirements, notes that ratings and opinions in audit reports may be appropriate if they align with the needs and expectations of internal audit stakeholders and internal audit acknowledges the accompanying risks. In many instances, ratings and opinions in internal audit reports will be something management will not embrace. As stated in the proposed *Standards*, "Internal audit must develop an engagement conclusion. . . . Based on the conclusion, internal audit must issue a rating, or other indicator of the significance of the aggregated findings."

¶ 606 CHALLENGES WITH TYPICAL INTERNAL AUDIT ACTIVITIES FOR THE FUTURE

Any discussion about challenges faced by internal audit must be considered with a focus on what traditional internal audit procedures have typically included, such as:

- Risk assessments and audit plan development
- Background gathering on the audit topic
- Entrance meeting for individual audits
- Interviews with business leaders
- Fieldwork, testing protocols, and reporting

Execution methods for each of these have been impacted by recent economic changes.

The main components of the current *IIA Standards* include:

- *Attribute Standards*, which address the characteristics of organizations and parties performing internal audit activities
- *Performance Standards*, which describe the nature of internal activities and provide criteria against which the performance of these services can be evaluated

As previously mentioned, the new proposed *Standards* do not use the categories of *Attribute Standards and Performance Standards*; however, the concepts therein are still incorporated throughout the new *Standards*.

Regardless of how or when the proposed *Standards* will become effective, the following are some of the major challenges internal auditors will face when trying to execute their responsibilities:

- Independence and objectivity, including organizational independence
- The CAE's role beyond internal auditing

- Due professional care
- Continuing professional development
- Internal assessment
- External assessment and reporting on the quality assurance review (QAR) program

Key to addressing the challenges is careful evaluation with management and the board. Internal auditors must be adaptable but still uphold their fiduciary duty.

Acknowledging these concepts and challenges, the proposed *Standards* have not gone through their stakeholder comment period. It will be up to the IIA to evaluate the concerns and comments of practitioners and make relevant changes. At the writing of this chapter, the expectation is that the new *Standards* will be effective by the end of 2023 with an expectation of a one-year grace period for implementation. Until then, the current IPPF framework is still in place as the guidelines for internal audit professionals. The remainder of this chapter discusses the current challenges faced by internal auditors outside of compliance with the *IIA Standards*.

¶ 607 EMERGING RISKS

Before examining other challenges created due to the pandemic and the economic environment, it is important to address emerging risk areas. Toward the end of 2019 and into 2021, many internal audit groups ranked the following as their top challenges:

- Emerging technologies
- Skillset
- Resources

With the onset of the pandemic and economic volatility, organizations, their environments, and their ways of working have evolved rapidly. The risks listed above are still challenges, yet they may have taken on a new meaning in the current environment.

The 10th annual "Executive Perspectives on Top Risks" survey (https://www.richardchambers.com/new-2022-top-risks-report-is-required-reading-for-internal-auditors/), a joint initiative by North Carolina State University's enterprise risk management (ERM) Initiative and Protiviti, outlined the top internal audit risks identified for 2022. The top seven risks indicated by survey respondents, which included more than 1,450 directors and executives worldwide, were the following:

- Pandemic-related government policies and regulation impacting business performance
- Succession challenges and the ability to attract and retain top talent
- Pandemic-related market conditions reducing customer demand
- Adoption of digital technologies requiring new skills or efforts to upskill/reskill employees
- Economic conditions, including inflationary pressures constraining growth opportunities
- Increasing labor costs impacting profitability targets
- Resistance to change operations and the business model

Another survey, the Audit Board's "2022 Focus on the Future," outlines the areas to which auditors are directing their efforts in 2022 to 2025 (https://www.auditboard.com/blog/critical-risk-areas-for-audit-efforts-2022/). According to this survey, cybersecurity and data privacy remains the highest risk category. Other top risks include finding and

retaining talent, third parties, regulatory changes, and business continuity and crisis response. These top five risks are consistent with those ranked by internal audit in the past.

Respondents to the Audit Board survey noted that audit teams plan to increase allocated resources to risks around artificial intelligence (AI), sustainability/climate change, and diversity, equity, and inclusion (DEI) by 2025. Also, several risk areas that were ranked *low* for 2022 are projected to have *higher risk assessments* in 2025. These include:

- Changing economic conditions
- Disruption of business
- DEI
- Sustainability and climate change
- Effectiveness of board oversight of management
- AI implementations

Emerging risks include disruption of business models, DEI, sustainability/climate change, and artificial intelligence. Those topics are cited as significant disruptors at meetings of executives and boards of directors. The Audit Board's survey results do not indicate that internal leaders believe these risks to be urgent enough to warrant extensive audit coverage at this time.

It is believed these results reflect cost versus benefit considerations. Internal audit must be capable of performing work on risks in the audit plan. Of the eleven skills included in the survey, eight are considered critical for improvement by at least a third of audit leaders. These skills include analytical/critical thinking, communications, cybersecurity, data mining/analytics, business acumen, risk management, and information technology (IT).

In essence, internal auditors can't audit what they do not understand. That means that once skill gaps are recognized, they need to be addressed and closed.

An interesting graphic in the survey outlined internal audit methods for upgrading skills and revealed a variance in upskilling current employees as it relates to technology-related versus non-technology-related skills.

Risk Actions

The "2022 Focus on the Future" survey outlined the following opportunities for internal audit leaders:

- Identify and prepare for emerging risks—sustainability/climate change, business model disruptions, AI, and DEI.
- Proactively address skill gaps.
- Leverage lessons learned from remote working.
- Expand use of technologies, including audit management and data analytics software.
- Build and maintain relationships with key stakeholders, whether they return to a central office or work remotely.

Internal auditors must work toward helping their organizations manage known and unknown risks. The fact that the traditional audit approach is retrospective in nature makes this concept difficult. As the need for business resiliency increases, internal auditors may be able to take on a role that provides a unique view of strategic risks. This goes beyond the audit plan and looks more broadly to explore the potential risks that could impact the organization.

This approach may be new to some. To effectively execute against this concept, internal auditors must be seen as proactive advisors to the organization while displaying a level of organizational skill and knowledge that is considered value added. In other words, internal audit must be seen as a value-add and not a retrospective check-and-balance function. This may require "educating" management and stakeholders regarding the evolving role of internal audit.

Some articles cite that internal auditors should step out of the box and be proactive, asking questions that are risk forward looking. However, the caution here is if management does not understand the reasoning for these actions and how they impact the audit plan, there may be negative reactions and consequences.

To be successful in adding to business resiliency and business risk mitigation, internal auditors must have a holistic understanding of the business environment and how current and emerging risks impact the organization.

The IIA suggests that one of the initial steps to becoming an integral part of a resilient organization is to proactively identify what is occurring in other areas. This means internal auditors must take part in innovation activities like steering committees, project management roles, working groups, and other initiatives (https://www.theiia.org/globalassets/documents/content/research/foundation/iaf-protiviti-business-resilience-report.pdf).

NOTE: According to the IIA, "The checklists of yesterday should not be dictating the plans for tomorrow."

Internal auditors have the opportunity to become strategic contributors in this area. If internal audit professionals are not willing to extend themselves beyond traditional boundaries and embrace changes, leadership will turn to other functions to fulfill those needs.

STUDY QUESTIONS

1. Under the new structure, which of the following domains focuses on the relationship between the board and the Chief Audit Executive (CAE)?

- **a.** Purpose of Internal Auditing
- **b.** Ethics and Professionalism
- **c.** Governing the Internal Audit Function
- **d.** Managing the Internal Audit Function

2. Under which of the following new domains do the *Standards* address how internal audit helps the organization serve the public interest?

- **a.** Purpose of Internal Auditing
- **b.** Ethics and Professionalism domain and Standards
- **c.** Governing the Internal Audit Function
- **d.** Performing Internal Audit Services

3. The proposed revisions to the *IIA Standards* were released in March 2023, and some concerns have been expressed. Which of the following is ***not*** one of those concerns?

- **a.** Use of the word *must* throughout the proposal
- **b.** Proposal relating to board of directors' responsibilities and internal audit
- **c.** The *Standards* mandating ratings or rankings for internal audit engagement findings
- **d.** Use of the word *shall* throughout the proposal

¶ 608 CHALLENGES

As organizations adapt to dealing with the impact of the COVID-19 pandemic and other economic challenges, internal auditors have an important role to play. They should continue to provide critical assurance; help advise management and the board on the shifting risk and controls landscape and help anticipate emerging risks.

The plans organizations are putting in place to contain and respond to the pandemic may be in place for quite some time. Therefore, the internal audit function should be prepared to adjust to this period in a sustainable way and adapt to this "new normal." Internal audit must identify the challenges that are in place and consider the following:

- Relevance of the current audit plan
- Ability to take a risk-balanced approach to future reviews
- Ability to provide assurance in the organization
- Ability to continue executing responsibilities while not disrupting critical operations
- Maintaining a corporate presence while working remotely
- Keeping staff motivated and supported
- Practicality of the current audit approach and audit cycle
- Need to assist on work that could challenge independence
- Ability to assess credibility of evidence when not on-site
- Ability to provide an objective voice and real-time assurance to teams that need to make decisions quickly
- Ability to timely communicate with management, stakeholders, and the audit committee
- If nonessential internal audit work is deferred, identifying the impact this has in meeting regulatory and statutory requirements

In these challenging times, internal audit executives have an obligation to help their companies manage the most critical risks. They can help management weigh risks and opportunities to inform their decisions. PricewaterhouseCoopers (PWC) released a white paper outlining areas where internal audit could assist management during these difficult times (https://www.pwc.com/us/en/library/covid-19/internal-audit.html). It reported that in the early part of the pandemic, 4 in 10 internal audit functions had redirected staff to put aside normal audit work to assist the organization by doing non-audit work. Key takeaways identified by PWC included the following actions by internal audit:

- Support the business to emerge stronger.
- Respond with flexibility and creativity.
- Help, not hinder.
- Use downtime to build for the future.

Internal auditors have seen a fundamental shift in the way their day-to-day processes work. This includes everything from the way they communicate with their team and stakeholders to how they execute their day-to-day responsibilities. In late

September 2021, the Audit Board published the results of its survey on how the pandemic had impacted internal audit (https://www.auditboard.com/blog/covid-impact-internal-audit/). It revealed the following five ways the pandemic has changed internal audit forever:

- The use of technology will be more critical to conducting internal audits in the future (91 percent of survey respondents agreed; 61 percent agreed strongly).
  - — The remote setback was mitigated through the use of technology.
  - — Department processes were automated by cloud-based platforms designed to facilitate remote collaboration.
- Internal auditors will be more focused on innovative means to gather and analyze evidence as part of internal audit processes (83 percent agreed; 34 percent agreed strongly).
  - — During the pandemic, risk and compliance teams mutually strategized to rely on each other's work.
  - — Video documentation and use of drones (for viewing physical assets) as well as the use of smart devices and video capabilities increased internal audit's reach.
- Most face-to-face meetings will be replaced with virtual meetings using video streaming technology (72 percent agreed; 26.3 percent agreed strongly).
  - — A recent survey revealed that the Zoom platform saw a 2,900 percent increase in usage since the end of 2019.
  - — The business world will increasingly embrace the hybrid work model.
  - — CAEs believe their teams will continue to rely heavily on technology-facilitated meetings as a more efficient means of communication.
- Internal auditors will focus more on emerging risks and their possible impacts on the company (72 percent agreed; 25.7 percent agreed strongly).
  - — Seventy-two percent of CAEs felt the dynamic nature and velocity of risks must be an overarching consideration for internal audit and other risk professionals.
  - — There must be a continuous method for assessing risks. This includes performing risk assessments with greater frequency.
  - — Internal auditors must enhance the methodologies and technologies relied on to create and maintain a continuous perspective on risks.
- Internal auditors will likely not return to traditional workplaces but will work remotely all or part of the time (68 percent agreed; 35 percent agreed strongly).
- A strong majority of CAEs will embrace flexible workplace arrangements in the future.
  - — The internal audit workplace of the future does not need to be exclusively in a traditional office setting.

How should internal auditors address these observations? PWC (https://www.pwc.com/my/en/publications/2020/internal-audit-adding-value-in-the-business-response-to-covid-19.html) offers the following recommendations:

- Redirect risk expertise to organization priorities.
- Identify ways to add value.
- Proactively communicate with all management, stakeholders, and the board about the impact of COVID-19 on internal audit resources and the audit plan.

- Consider redirecting any short-term capacity to activities that may assist the business at a strategic level.
- Evaluate emerging risks of newer operating models and business practices and redirect your attention to the most time-sensitive risks.
- Understand COVID-19's impact on your industry and business.
- Help manage regulator expectations by coordinating with the appropriate stakeholders.
- Provide leadership and support for compliance frameworks, processes, and control activities for COVID-19–related non-traditional funding (government stimulus or CARES Act).
- Reprioritize internal audit activities. Ask key questions:
  - — What projects can be stopped or delayed?
  - — What projects are still important and can be conducted remotely?
  - — Do we understand and have a handle on mandatory projects to meet regulatory requirements?
  - — Which projects should we add to address the new business and risk climate?
  - — Have we considered the cost/benefit of allocating internal audit time to external audit activities?
  - — Do we have the relevant resources and skills to do the work required by the organization?
  - — What outsource specialty skills are needed?

¶ 609 ADDRESSING CHALLENGES

It is clear the internal audit function will have to evolve and adapt just like other roles in the organization. Internal auditors should consider the following when addressing internal audit challenges:

- Evaluate priorities and identify critical work to ensure your team has focus on the greatest risks.
- Think of ways to keep things moving where an audit or other activity is business critical.
- Don't lose your focus.
- In a time of change and uncertainty, there may be instances of control override and employees may seek workarounds.
  - — Fraud risks may change as new opportunities are enabled for both internal and external parties.
  - — This may be an emerging area for increased monitoring by internal audit.
- Identify ways to transform the internal audit function to embrace a new flexible environment. This includes:
  - — Advancing governance methodologies like environmental, social, and governance (ESG)
  - — Enabling technologies such as AI and robotic process automation (RPA)
  - — Establishing a presence in ERM initiatives and understanding emerging risk areas
  - — Keeping an eye on the ever-changing global environment and understanding impacts and linkages to your organization. Find ways to embed findings into management reports and risk analysis

- Reprioritize/understand the increased risk and threat of the "new normal," including increased cyber presence.
  - With the rapid onset of the pandemic, immediate shutdowns, and continued flux of working situations, employees were forced into a work-at-home situation.
  - It is estimated that technology processes have advanced significantly in the past two years simply due to a requirements need.
  - With flexible working arrangements, user access controls may be compromised, and conflicts of interest may arise.
  - Cyber risk has escalated multifold in the past two years. If your organization was not properly prepared for cyber risks prior to the pandemic, this is a critical risk area to focus on.

There are many areas internal audit could evaluate and prioritize:

- Current management and internal audit monitoring techniques
- Segregation of duties rules while maintaining an audit trail
- Fraud detection risks and management overrides
- Changes, temporary or permanent, that are being made to the organization's internal control environment, with a specific focus on:
  - Management review controls
  - Accounting judgment controls
  - Transaction processing controls
  - Cash payments controls
  - Automated business controls
  - Outsource service providers
  - Key person dependency/super user access
  - Resilience and remote working

Risk Management

Technological advances in risk management software can help internal auditors move forward and be proactive and responsive, but tools are not the full answer. Internal auditors should strive beyond the third line of defense responsibilities as defined in the IIA's Three Lines of Defense Model. It will be imperative to find avenues to become engaged with management and the board on strategy and risk issues.

As remote work and use of third-party software increases, controls around business security may inadvertently be compromised. Internal auditors could evaluate whether remote access controls are built to scale, determine if third-party security plans have been adequately vetted, and examine service-level agreements to ensure they properly address risks. For risk management, internal auditors could:

- Evaluate the efficiency of ongoing processes to continue to meet regulatory responsibilities.
- Examine the risk assessment process and determine the need to become more agile and adopt more dynamic methodologies.

Cybersecurity

With regard to cybersecurity, internal auditors could:

- Examine if appropriate awareness and threat detection have been raised to proactively address potential malicious activity.
- Evaluate if adequate licenses are in place to cover greater use of tools, technology, and software.
- Examine the use of collaboration tools and other SaaS applications and ensure they are being monitored.
- Be an advocator for continuing education for employees on cybersecurity related issues.

Business Continuity

From a business continuity perspective, internal auditors could:

- Assist the business in identifying single points of failure (e.g., processes, employees, technologies).
- Develop and/or test appropriate scenarios, plans, or measures to restore business operations.
- Challenge management's forecasts of business impact (e.g., going concern, goodwill, expected credit losses).
- Examine management's assessment, monitoring, and contingency plans of key outsource service providers.

Operations and Supply

Regarding the supply chain, internal auditors could:

- Assess the sufficiency of resources to maintain critical activities at sufficient levels.
- Evaluate how the organization understands and prepares for changes in demand while balancing available resources.
- Internal auditors could also evaluate key contractual clauses that may offer relief, such as force majeure, notice provisions, limitation of liability, and more.

Finance and Liquidity

Related to finance, internal auditors could:

- Understand working capital requirements and assess cash flow.
- Monitor debt covenants.
- Evaluate critical path activities and assess resource requirements.
- Identify breached risk thresholds related to budgets and expenditures.
- Evaluate the organization's ability to access government fiscal support.
- Evaluate the organization's compliance with government fiscal support conditions.

Strategy and Brand

Strategies are often set in good times but tested in uncertain times. The pandemic is requiring leaders to review their strategies. It is important to prepare now for what might come next. In this vein, internal auditors could:

- Monitor and report on management strategy goals and processes.
- Monitor proposed growth and profitability projections through scenario planning and models that incorporate economic impacts of pandemics.
- Accelerate digital transformations.

IIA Recommendations

In a recent survey (https://www.theiia.org/globalassets/documents/content/research/foundation/iaf-protiviti-business-resilience-report.pdf), the IIA outlined important actions for internal auditors as they move forward and continue to navigate difficult economic times:

- Embed resilience into audit objectives.
- Be involved in process transformations, system implementations, and organizational transformations.
- Serve in an advisory capacity, including the facilitation of solutioning sessions, and establishing and reporting on metrics.

¶ 610 SKILLS

For the internal audit function to continue to thrive, there must be a focus on the internal auditor's skillset. Although each organization and industry has unique needs, generic areas to pursue include advanced analytics, machine learning, and communications. These skills are required for internal auditors to remain relevant.

Internal audit can work toward ensuring their employees have the right competencies by acknowledging technology. The use of technology and data are critical to a successful future. Staff must be ready to use and accept new tools. Internal audit teams should ask themselves several questions:

- What new tools and technologies should we embrace to stay on the leading edge of innovation?
- What is our plan for developing leadership roles in our organization?
- What talent, skills, and abilities do we need internally, and what is available externally?

Internal audit teams also should define how to build an understanding of each of these needs and specify a timeline in which their actions can be executed. Other recommendations due to the changing conditions of the workforce include the following:

- Keep employees safe, engaged, and productive. Help employees stay safe and healthy whether at work or home.
- Lead with responsive, empathetic communications and policies.
- Maintain the continuity of work by providing employees with the resources and support they need to be productive.
- Align workforce planning with your business strategy so you'll be ready to ramp up in a recovery.
- Maintain effective communications with your team.
- Conduct daily briefings or check-in routines.
- Assign personal mentors to help employees stay connected.
- Find ways to motivate employees remotely.
- Find ways to increase the number of progress updates given to key stakeholders across the business.
- Continue to develop strong relationships with clients around trust, credibility, efficiency, and transparency.

IA Staffing in the Future

The Audit Board has reported that internal audit resources increased in 2021 and are expected to increase even more by 2025 (https://www.auditboard.com/blog/critical-risk-areas-for-audit-efforts-2022/). Roughly half of those surveyed expect staff and budget increases over the next 12 to 24 months, while only a few anticipate declines. Skill sets identified where internal audit functions desire to upskill their staff are analytical/critical thinking/business acumen, risk management, and IT and cybersecurity.

Technology

The Audit Board's survey also identified that adoption of technology has made remote operations more effective. More than 80 percent of internal auditors expanded their use of specific technologies to enhance their work. They are relying more on data extraction/advanced analysis and cloud-based audit management software.

Data analytics can be performed regardless of location to provide planning information, audit evidence, and business insight. Cloud-based audit management software helps teams coordinate activities, combine insights, create a single source of record, and consolidate reporting. The internal audit function is expected to find long-term benefits from these improvements, even after life moves closer to pre-COVID norms.

The IIA resiliency report (https://www.theiia.org/globalassets/documents/content/research/foundation/iaf-protiviti-business-resilience-report.pdf) cited that internal audit should embrace digital transformation, innovation, and culture. For internal auditors to develop, they must stay in the forefront of new technologies and embrace new concepts such as dynamic risk assessments (using technology), data mining, and robotic process automation. This may require an adjustment to audit methodologies and protocols, and lack of acceptance may render internal audit obsolete.

Next-generation internal audit functions have moved beyond annual or quarterly risk updates. Processes are in place to timely recognize emerging risks and changes and incorporate them into the audit plan timely. Technology is the enabler.

It is anticipated that the future will bring greater acceptance and use of AI, robotic process automation (RPA), and machine learning, but many internal audit groups currently do not have all of these proficiencies in place. Those that do not have these capabilities should begin speaking to management now to identify the organization's future needs.

Internal audit should develop plans to highlight the need for these skills to management and the board. They should discuss whether the organization's recruiting for the talent needed in the future is adequate and whether management and Human Resources understand the types of skills needed.

Although technology skills are on the forefront of needed skillsets for auditors, that doesn't mean that audit teams will eliminate those who do not understand technology. Education is key.

The internal audit function also must be on the forefront of accepting and embracing change, being proactive in skill gap analysis, and providing timely and relevant training to staff on needed technological (and nontechnological) skills that will be required in the new normal. This process should be embedded within internal audit's annual review procedures.

¶610

¶ 611 SUMMARY

The past few years have certainly been complicated for all businesses and professionals, and many are still searching for answers. Those answers will evolve as more time passes and we recognize the full impact of the pandemic on all areas of a business. Although readers can incorporate many of the concepts discussed in this chapter in their move-forward strategy, it is important to stay abreast of emerging risks and remain agile in this changing environment. It is also important to stay abreast of the impending changes to the *IIA Standards*.

STUDY QUESTIONS

4. Which of the following was noted as the top risk area based on the 10th annual "Executive Perspectives on Top Risks"?

a. Succession challenges and the ability to attract and retain top talent

b. Pandemic-related government policies and regulation impacting business performance

c. Resistance to change operations and the business model

d. Increasing labor costs impacting profitability targets

5. Which of the following statements is correct with respect to addressing challenges?

a. In a time of change and uncertainty, there may be instances of control override.

b. It is not clear whether the internal audit function will have to evolve and adapt just like other roles in the organization.

c. Internal auditors must understand the reduced risk of cyber presence.

d. It is estimated that technology processes have advanced slightly in the past two years.

6. For internal audit to continue to thrive, there must be a focus on certain skills. Which of the following is ***not*** one of the skills mentioned?

a. Technology

b. Automation

c. Skillset

d. Audit checklists

CPE NOTE: When you have completed your study and review of chapters 4-6, which comprise Module 2, you may wish to take the Final Exam for this Module. Go to **cchcpelink.com/printcpe** to take this Final Exam online.

¶ 10,100 Answers to Study Questions

¶ 10,101 MODULE 1—CHAPTER 1

1. a. ***Incorrect.*** Instead, note that ESG concepts are a set of standards for an organization's operations (not its financial statements).

b. ***Incorrect.*** The standards include three central factors measuring sustainability and society impact of an investment.

c. ***Correct.*** **A 2020 survey by SustainAbility found that ESG ratings are the most frequently referenced source of information that institutional investors rely on to gauge ESG performance (55 percent, tied with direct company engagement).**

d. ***Incorrect.*** The ESG ratings industry is highly fragmented with dozens of ratings agencies and data providers in existence.

2. a. ***Incorrect.*** The percentage of respondents in the 2021 Statista survey who felt that environmental issues are a top risk or opportunity factor was greater than 40 percent.

b. ***Incorrect.*** This is the incorrect percentage of 2021 Statista survey respondents who reported that environmental issues are a top risk or opportunity factor. Note that the environment has been a focus of investors and stakeholders for many years.

c. ***Correct.*** **The correct percent is 79 percent. Also note that in April 2022, the CEO of Mastercard announced the company would offer sustainability-linked pay to all employees.**

d. ***Incorrect.*** The correct percentage is less than 85 percent. Also note that COSO approved a study to develop supplemental guidance and insights to its authoritative 2013 Internal Control Framework in the areas of sustainability and ESG.

3. a. ***Correct.*** **This is not one of the key factors that exist in ESG's growth into mainstream corporate accountability. Instead, the key factors include materiality, transparency, and regulation.**

b. ***Incorrect.*** Materiality is one of the key factors. Materiality in accounting refers to the concept that all the material items should be reported properly in the financial statements.

c. ***Incorrect.*** Transparency is one of the key factors. This relates to providing greater clarity on how client money is invested.

d. ***Incorrect.*** Regulation is one of the key factors. This relates to both national and international threats (e.g., climate change).

4. a. ***Incorrect.*** Climate change refers to long-term shifts in temperature and weather patterns. Since the 1800s, human activities have been the main driver of climate change.

b. ***Incorrect.*** Waste reduction is the practice of using less material and energy to minimize waste generation and preserve natural resources.

c. ***Incorrect.*** Deforestation or forest clearance is the removal of a forest or strand of trees from land that is then converted to non-forest use.

d. ***Correct.*** **Also note that environmental pollution is the contamination of physical and biological components of the earth and its atmosphere.**

5. a. ***Incorrect.*** This extends from sovereigns' policymaking to the distribution of rights and responsibilities among different participants in corporations, including the board of directors, managers, shareholders, and stakeholders.

b. ***Correct.*** **S&P Global assesses companies' governance performance by assessing four factors. They are (1) structure and oversight, (2) code and value, (3) transparency and reporting, and (4) cyber risk and systems.**

c. ***Incorrect.*** For example, this includes such things as a corporation's purpose, the role and makeup of the board of directors, and shareholder rights.

d. ***Incorrect.*** One aspect relates to shareholders demanding better representation of women on corporate boards and in executive ranks.

6. a. ***Correct.*** **Stewardship can be thought of as the playbook (i.e., the responsible allocation, management, and oversight of capital, leading to sustainable benefits for the economy, the environment, and society).**

b. ***Incorrect.*** Greenwashing occurs when ESG investment products are sold as a solution to address a sustainable issue.

c. ***Incorrect.*** Biodiversity refers to a measure of variation at the genetic, species, and ecosystem level.

d. ***Incorrect.*** This is the incorrect term. Note that companies will need to provide greater visibility into their operations related to labor practices, health and safety, and human rights.

¶ 10,102 MODULE 1—CHAPTER 2

1. a. ***Incorrect.*** Data on the blockchain is stored in "blocks," and these blocks are cryptographically connected in a linear chain.

b. ***Incorrect.*** A token is a form of digital asset that is created using blockchain technology, for certain utilities or purposes.

c. ***Correct.*** **Data on the blockchain is accessible to the "nodes" that are connected to the network. Each node has a copy of the entire database, and it is the blockchain technology that connects these nodes and executes the consensus protocol, based on which transactions are validated and transmitted.**

d. ***Incorrect.*** Blockchain is a distributed, decentralized ledger where transactions are recorded and confirmed in a partial anonymous manner.

2. a. ***Incorrect.*** This is a disadvantage of using cryptocurrency. Another disadvantage is lack of segregation of duties, due to inappropriate permissions to the participants in the ecosystems.

b. ***Correct.*** **Another advantage of using cryptocurrency is tamper-free and irreversible record history, resulting in increased authenticity of data.**

c. ***Incorrect.*** This is a disadvantage of using cryptocurrency. Another disadvantage is the risk of incomplete information that could lead to inaccurate and unreliable reporting.

d. ***Incorrect.*** This is a disadvantage of using cryptocurrency. Another disadvantage is disintegrated systems that do not connect with blockchain without significant customization/integration.

3. a. ***Incorrect.*** Colombia was not the first country to adopt cryptocurrency as legal tender. Note that there are historical differences between cryptocurrency and real currency.

b. ***Incorrect.*** Germany was not the first country to adopt cryptocurrency as legal tender. Before the first country in question to adopt, Bitcoin was not required to be accepted as payment by law.

c. ***Correct.*** **El Salvador was the first country to adopt cryptocurrency as legal tender, starting in 2021. In doing so, every economic agent must accept it as payment.**

d. ***Incorrect.*** Canada was not the first country to adopt cryptocurrency as legal tender. Note that some countries have begun trials of central bank digital currencies.

4. a. ***Correct.*** **The useful life of an intangible asset is indefinite if that life extends beyond the foreseeable horizon—that is, there is no foreseeable limit on the period of time over which the asset is expected to contribute to the cash flows of the reporting entity.**

b. ***Incorrect.*** Digital assets meet the definition of intangible assets and would generally be accounted for under FASB ASC 350, *Intangibles—Goodwill and Other*.

c. ***Incorrect.*** Legal tender is specific to a jurisdiction. For example, the U.S. Code states, "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues."

d. ***Incorrect.*** Instead, inventory is purchased and held in the ordinary course of business, with the intent to sell. Inventory is recorded at the lower of cost and net realizable value (NRV).

5. a. ***Incorrect.*** After the impairment loss is recognized, the adjusted carrying amount (not the replacement cost) becomes the new accounting basis of the intangible asset.

b. ***Incorrect.*** An intangible asset with an indefinite useful life should be tested for impairment annually or more frequently if events or changes in circumstances indicate it is more likely than not that it is impaired.

c. ***Incorrect.*** To perform impairment testing, management should track the carrying values of their individual digital assets (or a divisible fraction of an individual unit).

d. ***Correct.*** **Also note that these types of indefinite-lived intangible assets are not subject to amortization.**

6. a. ***Correct.*** **Therefore, it is important for a firm to understand the level of effort necessary to gain the knowledge about the ecosystem (or relevant parts thereof) needed to make a reasoned client acceptance and continuance determination and competently perform the audit.**

b. ***Incorrect.*** An auditor's ability to obtain a robust understanding of the client and its environment, including its system of internal control, is critical to an effective risk assessment and audit response.

c. ***Incorrect.*** Instead, performing audits of digital assets may require a firm to update, or include additional oversight of, its existing system of quality control.

d. ***Incorrect.*** If one or more engagements in the digital asset environment are accepted, a firm may need to consider (not must consider) other potential updates to the quality control system.

¶ 10,103 MODULE 1—CHAPTER 3

1. a. ***Incorrect.*** Examples of pressures include, but are not limited to, a need to obtain additional debt or equity capital to remain competitive, management having a significant equity interest in the company, and third-party revenue or profit expectations.

b. ***Incorrect.*** Examples of opportunities include, but are not limited to, significant related-party transactions, key financial statement amounts being based on estimates, and domination of management by a single individual.

c. ***Correct.*** **Motivation is not one of the categories within the fraud triangle. Instead, the categories include pressures, opportunities, and rationalizations.**

d. ***Incorrect.*** Examples of rationalizations include, but are not limited to, history of violations of securities laws or other regulations by management, excessive interest by management in company's stock price, and frequent auditor–client disputes.

2. a. ***Incorrect.*** This is not the approximate percentage of data breaches from insiders. Instead, this is the percentage of data breaches from state-sponsored activities.

b. ***Correct.*** **This is the percentage of data breaches from insiders. Note that a much higher percentage of data breaches are caused by outsiders.**

c. ***Incorrect.*** This is not the approximate percentage of data breaches from insiders. Instead, this is the percentage of data breaches from accidental loss.

d. ***Incorrect.*** This is the approximate percentage of data breaches from outsiders. The next most frequent data breach comes as a result of accidents, at approximately 25 percent.

3. a. ***Incorrect.*** Scareware is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software.

b. ***Correct.*** **Locky was ransomware malware released in 2016. It was delivered by email with an attached Microsoft Word document that contains malicious macros.**

c. ***Incorrect.*** TeslaCrypt was a ransomware trojan. In its early forms, TeslaCrypt targeted game-play data for specific computer games. It is now defunct, and its master key was released by the developers.

d. ***Incorrect.*** The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

4. a. ***Incorrect.*** This is used to gain personal or business information, such as usernames, passwords, Social Security numbers, credit card numbers, etc. It is accomplished by using fraudulent e-mail messages that appear to come from legitimate businesses or government agencies.

b. ***Correct.*** **Smishing is similar to phishing and vishing, but it is done using text messages rather than phone calls or email. Criminals try to obtain information or try to load malware on the victim's computer.**

c. ***Incorrect.*** Vishing is similar to phishing, but it occurs over the phone rather than over the internet. Criminals try to obtain information or try to load malware on the victim's computer.

d. ***Incorrect.*** A sockpuppet is an online identity used for purposes of deception. The term originally referred to a false identity assumed by a member of an Internet community who spoke to, or about, themselves while pretending to be another person.

5. a. ***Correct.*** **Spoofing is commonly used by spammers to hide the origin of an e-mail. This compares to pharming, which is a virus or malicious software that is secretly loaded onto the victim's computer and hijacks the web browser.**

b. ***Incorrect.*** This is used to gain personal or business information, such as usernames, passwords, Social Security numbers, credit card numbers, etc. It is accomplished by using fraudulent e-mail messages that appear to come from legitimate businesses or government agencies.

c. ***Incorrect.*** Vishing is similar to phishing, but it occurs over the phone rather than over the Internet. Criminals try to obtain information or try to load malware on the victim's computer.

d. ***Incorrect.*** Smishing is similar to phishing and vishing, but it is done using text messages rather than phone calls or email. Criminals try to obtain information or try to load malware on the victim's computer.

6. a. ***Incorrect.*** CSC 1 relates to having an inventory of authorized and unauthorized devices. It does not relate to having continuous vulnerability assessment and remediation.

b. ***Incorrect.*** CSC 2 relates to having an inventory of authorized and unauthorized software. It does not relate to having continuous vulnerability assessment and remediation.

c. ***Incorrect.*** CSC 3 relates to having secure configurations for hardware and software on mobile devices, laptops, workstations, and servers.

d. ***Correct.*** **CSC 4 relates to having continuous vulnerability assessment and remediation. It is one of many CIS Critical Security Controls that are recommended cybersecurity controls.**

¶ 10,104 MODULE 2—CHAPTER 4

1. a. ***Incorrect.*** This SAS addresses the auditor's responsibilities in the audit of financial statements relating to the entity's ability to continue as a going concern and the implications for the auditor's report.

b. ***Incorrect.*** This SAS addresses the auditor's responsibility to form an opinion on the financial statements. It also addresses the form and content of the auditor's report issued as a result of an audit of financial statements.

c. ***Incorrect.*** This SAS addresses the auditor's responsibilities relating to other information, whether financial or nonfinancial information (other than financial statements and the auditor's report thereon), included in an entity's annual report.

d. ***Correct.*** **It was effective for periods ending, or for practitioners' examination or review reports dated, on or after December 15, 2020, respectively.**

2. a. ***Correct.*** **This statement delays the effective dates of SAS Nos. 134–140, and the amendments to other SASs made by SAS Nos. 134–140, from December 15, 2020, to December 15, 2021, in order to provide more time for firms to implement these SASs in light of the effect of the coronavirus pandemic.**

b. *Incorrect.* SAS No. 142 supersedes AU-C Section 500, *Audit Evidence*, and amends various other sections of SAS No. 122, *Statements on Auditing Standards: Clarification and Recodification*, as amended.

c. *Incorrect.* This SAS addresses the auditor's responsibilities relating to accounting estimates, including fair value accounting estimates, and related disclosures in an audit of financial statements.

d. *Incorrect.* Note that the correct SAS explains what constitutes audit evidence in an audit of financial statements and sets out attributes of information that are taken into account by the auditor when evaluating information to be used as audit evidence.

3. a. *Incorrect.* SAS No. 136 does not impact the reporting on financial statements of not-for-profit entities. Note that Exhibit B of the SAS provides transitional implementation reporting guidance upon initial implementation by the auditor of this SAS.

b. *Correct.* This SAS creates a new AU-C Section 703 in the AICPA *Professional Standards* and addresses the auditor's responsibility to form an opinion and report on the audit of financial statements of employee benefit plans subject to the Employee Retirement Income Security Act of 1974 (ERISA).

c. *Incorrect.* SAS No. 136 does not impact the reporting on financial statements of private entities. Note that this SAS creates a new AU-C Section 703 in the AICPA *Professional Standards*.

d. *Incorrect.* SAS No. 136 does not impact the reporting on financial statements of public business entities. Instead, it is applicable to entities that are subject to the Employee Retirement Income Security Act of 1974 (ERISA).

4. a. *Incorrect.* This SAS addresses the auditor's responsibilities in the audit of financial statements relating to the entity's ability to continue as a going concern and the implications for the auditor's report.

b. *Incorrect.* This SAS addresses the auditor's responsibility to form an opinion on the financial statements. It also addresses the form and content of the auditor's report issued as a result of an audit of financial statements.

c. *Correct.* This SAS addresses the auditor's responsibilities relating to other information, whether financial or nonfinancial information (other than financial statements and the auditor's report thereon), included in an entity's annual report.

d. *Incorrect.* SAS No. 138 amends various AU-C sections in the AICPA *Professional Standards*, to align the materiality definition with the description of materiality used in the U.S. judicial system, the auditing standards of the PCAOB, the SEC, and the FASB.

5. a. *Correct.* This section relates to the auditor's responsibilities relating to other information included in the annual report.

b. *Incorrect.* This section does not relate to required supplementary information. Instead, it relates to financial statements prepared in accordance with a financial reporting framework generally accepted in another country.

c. *Incorrect.* This section does not relate to required supplementary information. Instead, it relates to letters for underwriters and certain other requesting parties.

d. *Incorrect.* This section does not relate to required supplementary information. Instead, it relates to compliance audits.

6. a. ***Incorrect.*** This is the incorrect effective date for SAS No. 138. Note that the history of the concept of materiality dates back to 1867, when the English Court introduced the term *material* by referring to "relevant, not negligible fact" that emerged in the judgement of the false accounting case concerning the Central Railways of Venezuela.

b. ***Incorrect.*** This is the incorrect effective date for SAS No. 138. Instead, it is effective at a later date.

c. ***Incorrect.*** This was the original effective date for SAS No. 138. However, this effective date was delayed by SAS No. 141.

d. ***Correct.*** **This is the correct effective date for SAS No. 138. Regarding materiality, it has quickly become essential for stakeholder engagement exercises and topic mapping while appearing as a keyword in consultant pitches.**

¶ 10,105 MODULE 2—CHAPTER 5

1. a. ***Correct.*** **It aligns many of the underlying principles of the new lessor model with those in ASC Topic 606, the new revenue recognition standard (e.g., those related to evaluating when profit can be recognized).**

b. ***Incorrect.*** This ASU relates to the recognition of breakage for certain prepaid stored-value products (a consensus of the FASB Emerging Issues Task Force).

c. ***Incorrect.*** This ASU relates to the effect of derivative contract novations on existing hedge accounting relationships (a consensus of the FASB Emerging Issues Task Force).

d. ***Incorrect.*** This ASU relates to improvements to employee share-based payment accounting, not lease accounting.

2. a. ***Incorrect.*** Leases of intangible assets are not within the scope of ASC Topic 842. Leases to explore for or use minerals, oil, natural gas, and similar assets would also not be within the scope of ASC Topic 842.

b. ***Correct.*** **Leases of buildings would be within the scope of ASC Topic 842. Additionally, leases of machinery and equipment would also be in scope.**

c. ***Incorrect.*** Leases of biological assets are not within the scope of ASC Topic 842. Leases of assets under construction are also not within the scope of ASC Topic 842.

d. ***Incorrect.*** Leases of inventory are not within the scope of ASC Topic 842. Leases of intangible assets are also not within the scope of ASC Topic 842.

3. a. ***Incorrect.*** Instead, a lessee is required to classify a lease as a finance lease when it meets any one of the respective criteria (e.g., lease transfers ownership of the underlying asset to the lessee by the end of the lease term).

b. ***Incorrect.*** By contrast, "reasonably certain" is defined as a high degree of confidence (e.g., 85 to 90 percent) that an event will take place.

c. ***Incorrect.*** Lessees have an accounting policy option to recognize payments on a short-term lease on a straight-line basis over the lease term.

d. ***Correct.*** **Also note that if after a lessee has made the determination that a contract contains a lease, the company is required to identify separate lease components within the contract and consider the right to use an underlying asset to be a separate lease component if certain conditions are met.**

4. a. ***Incorrect.*** This is not the correct date. Note that when calculating lease payments, fixed payments less any lease incentives paid or payable to lessee should be included.

b. ***Correct.*** **This is a key date to keep in mind. In fact, you need to calculate the payment stream over the lease term to determine the present value of future minimum lease payments.**

c. ***Incorrect.*** This is not the correct date. However, one of the first questions to ask is whether or not the arrangement involves the use of an identified asset.

d. ***Incorrect.*** This is not the correct date. Note that there is a difference between service contracts and leases. Service contracts give rise to different rights and obligations compared to those of a lease contract.

5. a. ***Correct.*** **Lessees are required to present both qualitative and quantitative information about their leases, the significant judgments made, as well as the amounts recognized in the financial statements.**

b. ***Incorrect.*** ASC Topic 842 requires that both finance lease RoU assets and operating lease RoU assets be presented separately from other assets on the statement and in the footnotes.

c. ***Incorrect.*** Instead, operating leases should be included in income from continuing operations as a single lease cost.

d. ***Incorrect.*** The presentation requirements for cash outflows are aligned to the presentation of expenses arising from a lease in the income statement (e.g., payments arising from operating leases should be disclosed in cash flows from operating activities).

6. a. ***Incorrect.*** This is a procedure that should be performed. You should also test the clerical accuracy of the analysis.

b. ***Incorrect.*** This is a procedure that should be performed. You should also review any reconciliation to the general ledger and investigate any unusual reconciling items.

c. ***Incorrect.*** This is a procedure that should be performed. You should also determine that significant related-party leases are classified and accounted for on the basis of the legally enforceable terms and conditions of the lease in the same manner as leases between unrelated parties.

d. ***Correct.*** **A RoU asset is not recorded for short-term leases. A short-term lease is a lease that at the commencement date has a lease term of 12 months or less and does not include an option to purchase the underlying asset that the lessee is reasonably certain to exercise, will not be recorded on the balance sheet.**

¶ 10,106 MODULE 2—CHAPTER 6

1. a. ***Incorrect.*** This is one of the five new domains proposed. However, this domain contains elements of the current Definition/Mission of Internal Audit.

b. ***Incorrect.*** This is one of the five new domains proposed. However, this domain incorporates and builds upon the current Code of Ethics.

c. ***Correct.*** **Under the new structure, there is content from six elements of the current IPPF (Mission, Definition, Code of Ethics, Core Principles, Standards, Implementation Guides) incorporated into five domains.**

d. ***Incorrect.*** This is one of the five new domains proposed. However, this domain focuses on requirements for CAEs to effectively manage internal auditors.

2. a. *Correct.* The first domain in the new *Standards* incorporates the Mission of Internal Audit and the Definition of Internal Audit, and for the first time, addresses how internal audit helps the organization serve the public interest.

b. *Incorrect.* The Code of Ethics has been incorporated into the Ethics/Professionalism domain and contains information about due professional care, professional skepticism, etc.

c. *Incorrect.* In this domain, the definition/use of the term *board* and the board's role in governing the internal audit function has been clarified.

d. *Incorrect.* This new domain focuses on performing assurance and advisory engagements.

3. a. *Incorrect.* This is one of the concerns expressed by stakeholders. Also note that the future of work for internal auditors will require adapting to new technologies, collaborating with other functions, and being more strategic in their approach.

b. *Incorrect.* This is one of the concerns expressed by stakeholders. It's important to note that any discussion about challenges faced by internal audit in recent times must be considered with a focus on what traditional internal audit procedures have typically included.

c. *Incorrect.* This is one of the concerns expressed by stakeholders. The proposed *Standards* would also require a rating for the aggregated engagement results.

d. *Correct.* This is not one of the concerns expressed by stakeholders. Instead, one of the concerns relates to the use of the word *must* throughout the proposal.

4. a. *Incorrect.* Succession challenges and the ability to attract and retain top talent was a risk that was noted, but it was not the top risk.

b. *Correct.* The 10th annual "Executive Perspectives on Top Risks" (a joint initiative by NC State University's ERM Initiative and Protiviti) noted this as a top risk.

c. *Incorrect.* This was a risk noted by the survey, though not the top risk. Also note that the Audit Board's "2022 Focus on the Future" survey outlines the areas auditors are directing their efforts to in 2022 to 2025.

d. *Incorrect.* This was a risk noted by the survey, though not the top risk. Note that the survey included more than 1,450 directors and executives worldwide.

5. a. *Correct.* Internal auditors shouldn't lose their focus. In a time of change and uncertainty, there may be instances of control override and employees may seek workarounds.

b. *Incorrect.* Instead, it is clear the internal audit function will have to evolve and adapt just like other roles in the organization.

c. *Incorrect.* Internal auditors must reprioritize/understand the increased risk and threat of the "new normal" including increased cyber presence.

d. *Incorrect.* Instead, it is estimated that technology processes have advanced significantly in the past two years simply due to a requirements need.

6. a. ***Incorrect.*** Technology is an important aspect of an internal audit and should be a focus for internal audit to continue to thrive.

b. ***Incorrect.*** Automation is an important aspect of internal audit. Automation is the use of technology to perform tasks where human input is minimized.

c. ***Incorrect.*** Each organization and industry has unique needs. Some generic areas to pursue include advanced analytics, machine learning, and communications**.**

d. ***Correct.*** **Audit checklists are a thing of the past and should not necessarily be an area of focus in the future.**

Index

References are to paragraph (¶) numbers.

D

E

F

G

I

K

L

¶ 10,200 Glossary

Algorithm: A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

Attribute Standards: Standards that address the characteristics of organizations and parties performing internal audit activities.

Auditing Standards Board: The senior technical committee designated by the American Institute of Certified Public Accountants (AICPA) to issue auditing, attestation, and quality control statements, standards, and guidance to certified public accountants for non-public company audits.

Biodiversity: A measure of variation at the genetic, species, and ecosystem level.

Blockchain: A distributed, decentralized ledger where transactions are recorded and confirmed in a partial anonymous manner.

Climate Change: Long-term shifts in temperatures and weather patterns.

Cryptocurrency: A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.

Cryptography: The art of writing or solving codes.

Cybersecurity: The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Deforestation: The removal of a forest or strand of trees from land that is then converted to non-forest use.

DEI: Diversity, equity, and inclusion.

Distributed Ledger Technology (DLT): A consensus of shared, digital data that is geographically spread across multiple sites, countries, or institutions. Blockchain is a type of DLT.

Encryption: Conversion of data to another format that cannot be read or viewed until it is decrypted.

Environmental Pollution: The contamination of physical and biological components of the earth and its atmosphere.

Environmental Sustainability: The responsibility (related to the planet) to maintain natural resources and avoid adversely impacting the ability for future generations to meet their needs.

ESG: Environmental, social, and corporate governance; an approach to evaluating the extent to which a corporation works on behalf of social goals that go beyond the role of a corporation to maximize profits on behalf of the corporation's shareholders.

ESG Integration: Incorporates all material ESG factors in investment analysis and decisions to determine the potential impact on the company performance.

ESG Rating: A rating that is calculated based on a company's material exposure to company-specific and general-industry ESG risk, and how it manages those risks.

Fiat Currency: Legal currency that is generated by a sovereign government.

Finance Lease: From the perspective of a lessee, a lease that meets one or more of the criteria in paragraph 842-10-25-2 of Accounting Standards Update (ASU) Topic 842.

Fraud: An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right.

Fraud Triangle: A framework designed to explain the reasoning behind a worker's decision to commit workplace fraud.

Going Concern: A term for a company that has the resources needed in order to continue to operate indefinitely.

Greenwashing: Occurs when ESG investment products are sold as a solution to address a sustainable issue. This happens when the subsequent sustainable components' results are questionable.

Initial Direct Costs: Incremental costs of a lease that would not have been incurred if the lease had not been obtained.

Inquiry: Consists of seeking information of knowledgeable persons within or outside the entity.

Institute of Internal Auditors (IIA): A certification, education, and research leader for professionals engaged in evaluating an organization's operations and controls.

Internal Audit: An independent, objective assurance and consulting activity designed to add value to and improve an organization's operations.

Key Audit Matters (KAMs): Those matters that were communicated with those charged with governance and, in the auditor's professional judgment, were of most significance in the audit of the financial statements of the current period.

Lease: A contract, or part of a contract, that conveys the right to control the use of identified property, plant, or equipment for a period of time in exchange for consideration.

Lease Modification: A change to the terms and conditions of a contract that results in a change in the scope of or the consideration for a lease (e.g., a change to the terms and conditions of the contract that adds or terminates the right to use one or more underlying assets or extends or shortens the contractual lease term).

Lease Term: The noncancellable period for which a lessee has the right to use an underlying asset plus periods covered by an option to extend the lease if the lessee is reasonably certain to exercise that option, periods covered by an option to terminate the lease if the lessee is reasonably certain not to exercise that option, and periods covered by an option to extend (or not to terminate) the lease in which exercise of the option is controlled by the lessor.

Machine Learning: A field devoted to understanding and building methods that let machines "learn"—that is, methods that leverage data to improve computer performance on some set of tasks.

Malware: Software that is placed on computers or cell phones to hijack the computers, steal data, or encrypt the data for ransom.

Materiality: A concept or convention within auditing and accounting relating to the importance/significance of an amount, transaction, or discrepancy.

Node: A copy of the ledger, containing a complete record of all the transactions recorded on the blockchain and operated by a participant of the blockchain network.

Off-chain Transactions: Blockchain-based cryptocurrency transactions that occur outside of the blockchain network.

On-chain Transactions: Blockchain-based transactions that occur when processed and successfully broadcast on the blockchain network.

¶10,200

Operating Lease: From the perspective of a lessee, any lease other than a finance lease. From the perspective of a lessor, any lease other than a sales-type lease or a direct financing lease.

Performance Standards: Describe the nature of internal audit activities and provide criteria against which the performance of these services can be evaluated.

Phishing: A technique used by fraudsters to obtain personal information for the purpose of identity theft. This theft can include sending illegitimate emails asking for personal information.

Private Blockchain: A blockchain managed by a single entity (or a group of entities), based on certain rules/consensus. The network is closed; only those with permission can participate.

Professional Skepticism: An attitude that includes a questioning mind, being alert to conditions that may indicate possible misstatement due to fraud or error, and a critical assessment of review evidence.

Public Blockchain: A distributed, open, and decentralized ledger of encrypted information, where participants can read, write, and view data.

Skillset: A person's range of skills or abilities.

Smishing: Fraud that is similar to phishing and vishing, but it is done using text messages rather than phone calls or email.

Spoofing: A term used to describe fraudulent email activity in which the sender's address or other parts of the email header are altered to appear as though the email originated from a different source.

Stranded Assets: Assets that, at some point prior to the end of their economic life, become more worthless than anticipated due to the transition to a low-carbon economy (creating lower-than-expected demand or prices).

Substantial Doubt: In management's judgment, it is probable that the client will not continue as a going concern.

Token: A form of digital asset that is created using blockchain technology, for certain utilities or purposes.

Vishing: Fraud that is similar to phishing but is done over the phone rather than through email.

Waste Reduction: The practice of using less material and energy to minimize waste generation and preserve natural resources.

¶ 10,300 Final Exam Instructions

To complete your Final Exam go to **cchcpelink.com/printcpe**, click on the title of the exam you wish to complete and add it to your shopping cart (you will need to register with CCH CPELink if you have not already). Click **Proceed to Checkout** and enter your credit card information. Click **Place Order** to complete your purchase of the final exam. The final exam will be available in **My Dashboard** under **My Account**.

This Final Exam is divided into two Modules. There is a grading fee for each Final Exam submission.

Online Processing Fee:	**Recommended CPE:**
$144.00 for Module 1	6 hours for Module 1
$120.00 for Module 2	5 hours for Module 2
$264.00 for both Modules	11 hours for both Modules

Instructions for purchasing your CPE Tests and accessing them after purchase are provided on the **cchcpelink.com/printcpe** website. **Please note, manual grading is no longer available for Top Accounting and Auditing Issues. All answer sheets must be submitted online for grading and processing.**

Recommended CPE credit is based on a 50-minute hour. Because CPE requirements vary from state to state and among different licensing agencies, please contact your CPE governing body for information on your CPE requirements and the applicability of a particular course for your requirements

---

Expiration Date: September 30, 2025

Evaluation: To help us provide you with the best possible products, please take a moment to fill out the course Evaluation located after your Final Exam.

Wolters Kluwer, CCH is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.learningmarket.org.

Additional copies of this course may be downloaded from **cchcpelink.com/printcpe**. Printed copies of the course are available for $15.00 by calling 1-800-344-3734 (ask for product 10024493-0011).

¶ 10,301 FINAL EXAM QUESTIONS: MODULE 1

1. The concept of ESG focuses primarily on how many elements?

a. One

b. Three

c. Four

d. Five

2. Which of the following provides an objective measurement or evaluation of a company, fund, or security's performance with respect to ESG issues?

a. ESG Rank

b. ESG Score

c. ESG Rating

d. ESG Grade

3. Which of the following organizations approved a study to develop supplemental guidance and insights to its authoritative 2013 Internal Control Framework in the areas of sustainability and ESG?

a. FASB

b. IASB

c. COSO

d. SEC

4. What percentage of the respondents to a 2021 survey by Statista stated that environmental issues are a top risk or opportunity factor in their view?

a. 14 percent

b. 23 percent

c. 51 percent

d. 79 percent

5. Which of the following identifies the gradual thinning of the Earth's ozone layer in the upper atmosphere?

a. Ozone depletion

b. Deforestation

c. Green washing

d. Pollution

6. At its core, the _____ component of ESG is about human rights and equity—an organization's relationships with people, as well as its policies and actions that impact individuals, groups, and society.

a. Governance

b. Social

c. Environmental

d. Societal

7. S&P Global Market Intelligence research revealed firms with more women on their board of directors and in C-suite positions had _____ financial performance than less diverse companies.

- **a.** The same
- **b.** Reduced
- **c.** Slightly reduced
- **d.** Greater

8. When considering ESG approaches, investors must recognize the underlying themes that are producing some of the key risk factors within ESG investing. Which of the following themes encompasses unequal access to the benefits of belonging to any society?

- **a.** Climate change
- **b.** Biodiversity
- **c.** Social inequality
- **d.** Supply chain management

9. Which of the following identifies the first step in establishing an ESG program?

- **a.** Determine business-specific ESG issues
- **b.** Evaluate existing programs
- **c.** Set goals and create a framework for ESG
- **d.** Develop actionable plans and key performance indicator measurements

10. The Center of Audit Quality (CAQ) found that what percentage of S&P 500 companies had detailed ESG information publicly available primarily outside of a Securities and Exchange Commission (SEC) submission?

- **a.** 24 percent
- **b.** 37 percent
- **c.** 61 percent
- **d.** 95 percent

11. Data on the blockchain is stored in which of the following?

- **a.** Nodes
- **b.** Blocks
- **c.** Wallets
- **d.** Keys

12. According to recent statistics, the total crypto market cap was more than which of the following?

- **a.** $2 trillion
- **b.** $4 trillion
- **c.** $6 trillion
- **d.** $9 trillion

13. Which of the following represents the right to ownership of a unique intangible asset on the blockchain and symbolizes the digital creation of a real-world asset?

- **a.** Nodes
- **b.** Blocks
- **c.** Non-fungible tokens
- **d.** Smart contracts

14. Which of the following identifies long strings of random alphanumeric cryptographic code that are generated by the blockchain?

a. Nodes

b. Wallets

c. Blocks

d. Keys

15. Which of the following is a disadvantage of using crypto?

a. Inappropriate wallet access rights

b. Increased security

c. Real-time transaction updates

d. Reduced processing time

16. Which of the following organizations participated in a joint statement in January 2023 highlighting key risks associated with crypto assets that could affect banks?

a. FASB

b. OCC

c. SEC

d. IRS

17. Which of the following organizations released a guide for the accounting and auditing of digital assets?

a. FASB

b. SEC

c. AICPA

d. IASB

18. Which of the following is ***not*** one of the four major classes of assets under current U.S. GAAP guidance?

a. Cash and cash equivalents

b. Inventory

c. Financial instruments

d. Comprehensive income

19. The initial recognition of digital assets should follow the guidance prescribed by which of the following ASC Topics?

a. ASC Topic 280

b. ASC Topic 350

c. ASC Topic 606

d. ASC Topic 842

20. If an entity relies on a third-party custodian to store its digital assets, the auditor considers additional risks at which of the following?

a. At the entity only

b. Neither at the entity nor at the custodian

c. At the custodian only

d. At both the custodian and entity

21. The Rational Choice Theory notes in part that individuals choose when and where to commit fraud, and the higher the likelihood of getting caught or punished, the less likely they are to commit fraud. This theory was developed by Cornish and Clarke in what year?

a. 1981

b. 1986

c. 1991

d. 1999

22. Based on the 2022 ACFE Occupational Fraud report, which of the following types of occupational fraud represents the largest component on its own?

a. Asset misappropriation

b. Corruption

c. Financial statement fraud

d. Phishing

23. The number of complaints and value of losses reported by the Internet Crime Complaint Center over the last five years has done which of the following?

a. Decreased significantly

b. Increased

c. Decreased slightly

d. Stayed about the same

24. Each of the following identifies an IT system cybersecurity risk factor, ***except?***

a. Overtrained IT personnel

b. Complex IT systems

c. Older technology

d. Lack of internal controls

25. What percentage of data breaches is generally caused by outsiders?

a. 2 percent

b. 11 percent

c. 25 percent

d. 62 percent

26. Which of the following is the most frequent personally identifiable information (PII) attribute subject to data breaches?

a. Social Security number

b. Date of birth

c. Name

d. Home address

27. Which of the following is the first stage of a ransomware attack?

a. Reconnaissance and lateral movement

b. Data exfiltration and encryption

c. Ransom demand

d. Initial intrusion

28. Which of the following types of fraud is accomplished by using fraudulent email messages that appear to come from legitimate businesses or government agencies?

a. Vishing
b. Phishing
c. Smishing
d. Wishing

29. Keylogger, Win-Spy, Spytech Spy Agent, and SpectorSoft are examples of which of the following?

a. Spyware
b. Ransomware
c. Phishing
d. Malware

30. The NIST Framework for Improving Critical Infrastructure Cybersecurity includes five key components. Which of the following is the first component in the process?

a. Protect
b. Detect
c. Identify
d. Respond

¶ 10,302 FINAL EXAM QUESTIONS: MODULE 2

1. Which of the following SASs was issued in May 2019 to improve the transparency and relevance of the communication in the auditor's report?

a. SAS No. 134
b. SAS No. 135
c. SAS No. 136
d. SAS No. 137

2. Which of the following is a characteristic/change with respect to SAS No. 134?

a. The auditor's report is moved to the last section of the report.
b. The Basis for the Opinion section is at the front of the report.
c. The section related to the auditor's responsibilities was not changed.
d. The Basis for the Opinion section is new.

3. Section 701 was added as a result of SAS No. 134 to address which of the following?

a. Key audit matters
b. Subsequent events
c. Going concern
d. Goodwill impairment

4. The primary focus of SAS No. 135 was amending each of the following AU-Cs, ***except?***

a. AU-C Section 240
b. AU-C Section 260
c. AU-C Section 550
d. AU-C Section 855

5. Which of the following SASs relates to forming an opinion and reporting on financial statements of employee benefit plans subject to ERISA?

a. SAS No. 135
b. SAS No. 136
c. SAS No. 137
d. SAS No. 138

6. Subsequent to the release of SAS No. 136, which of the following types of audits will now be referred to as an "ERISA Section 103(a)(3)(C)" audit?

a. Modified scope
b. Full scope
c. Limited scope
d. Risk-based scope

7. Which of the following SASs is expected to reduce diversity in practice and improve transparency related to the auditor's responsibilities for other information and documents that are within the scope of the standard?

a. SAS No. 137
b. SAS No. 138
c. SAS No. 139
d. SAS No. 140

8. Searching for omitted or incomplete information _____ required of the auditor based on SAS No. 137.

a. Is
b. May be
c. Is not
d. Always is

9. SAS No. 138 addressed which of the following key auditing concepts?

a. Materiality
b. Sampling
c. Acceptable risk
d. Going concern

10. Delaying the effective dates of SAS Nos. 134 through 140 provided relief to public accounting firms amid the challenges created by which of the following?

a. The new audit reporting model
b. The stock market
c. The COVID-19 pandemic
d. The financial crisis

11. The new lease standard aligns many of the underlying principles of the new lessor model with which of the following ASC Topics?

a. ASC Topic 280
b. ASC Topic 450
c. ASC Topic 606
d. ASC Topic 958

12. Approximately what amount of right-of-use (RoU) assets and lease payment liabilities will be added on by U.S. companies' balance sheets on account of the new lease standard?

a. $1 trillion
b. $2 trillion
c. $3 trillion
d. $5 trillion

13. On June 3, 2020, the Financial Accounting Standards Board (FASB) issued which of the following Accounting Standards Updates which amended the effective date of the new leasing standard?

a. ASU 2020-01
b. ASU 2020-02
c. ASU 2020-05
d. ASU 2020-07

14. Which of the following identifies a contract, or part of a contract, that conveys the right to control the use of identified property, plant, or equipment for a period of time in exchange for consideration?

a. Rental
b. Service
c. Lease
d. Agency

15. In the FASB's view, a lessee's right to use the underlying asset meets the definition of which of the following?

a. A liability

b. An intangible

c. A security

d. An asset

16. A short-term lease is a lease that, at the commencement date has a lease term of ____ months or less and does not include an option to purchase the underlying asset that the lessee is reasonably certain to exercise.

a. 12

b. 18

c. 24

d. 36

17. Commissions or payments made to an existing tenant to terminate the lease are examples of which of the following types of costs?

a. Indirect costs

b. Facilitation costs

c. Initial direct costs

d. Termination costs

18. Operating leases should be included in income from continuing operations as which of the following?

a. A single lease cost

b. A variable lease cost

c. A depreciation cost

d. An amortization cost

19. ASC Topic 842 _____ change lease characterization for federal income tax purposes.

a. Does

b. May

c. Does not

d. Should

20. For any leases that were not tested in a prior audit or were significantly modified in the current period, an auditor should perform each of the following procedures, ***except?***

a. Estimate the amount of RoU assets not tested that should be disclosed within the auditor's report.

b. Obtain and review lease contracts and other applicable documents and review abstracts or copies of significant lease contracts analyzed in prior years.

c. Determine that the contracts contain a lease, and that the client has identified the separate lease components (or multiple components) and non-lease component.

d. Consider whether to confirm significant lease obligations and related lease provisions.

21. In what year did the Institute of Internal Auditors (IIA) undertake an extensive review to update its *Standards*?

a. 2018
b. 2019
c. 2020
d. 2021

22. At this time, the official release of the finalized update to the *IIA Standards* is scheduled for the end of which of the following years?

a. 2023
b. 2024
c. 2025
d. 2026

23. The *IIA Standards* are _____ focused and provide a framework for performing internal auditing.

a. Principles
b. Risk
c. Materiality
d. Fair value

24. Under the new structure in the proposed *IIA Standards*, content is incorporated into how many domains?

a. 4
b. 5
c. 6
d. 9

25. Which of the following domains of the IIA proposed *Standards* focuses on requirements for Chief Audit Executive to effectively manage internal audit?

a. Performing Internal Audit Services
b. Governing the Internal Audit Function
c. Ethics and Professionalism
d. Managing the Internal Audit Function

26. Some concerns have been expressed since IIA proposed revisions were released in March 2023, one of which is the use of the word _____ throughout the proposal.

a. May
b. Should
c. Must
d. Can

27. The Audit Board's "2022 Focus on the Future" survey outlines the areas auditors are directing their efforts to over what time period?

a. 2022 to 2023
b. 2022 to 2025
c. 2022 to 2029
d. 2022 to 2032

28. The "2022 Focus on the Future" survey outlined opportunities for internal audit leaders. One of these was to proactively address which kind of gap?

a. Compliance

b. Ethics

c. Skill

d. Responsibility

29. Cyber risk has escalated how much in the past two years?

a. Very little

b. Some

c. A decent amount

d. Multifold

30. The IIA resiliency report cited that internal audit should embrace digital transformation, innovation, and which of the following?

a. Culture

b. Diversity

c. Adaptability

d. Equity

¶ 10,400 Answer Sheets

¶ 10,401 Top Accounting and Auditing Issues for 2024 CPE Course: MODULE 1

Go to **cchcpelink.com/printcpe** to complete your Final Exam online for instant results.

A $144.00 processing fee will be charged for each user submitting Module 1 to **cchcpelink.com/printcpe** online for grading.

Module 1: Answer Sheet

Please answer the questions by indicating the appropriate letter next to the corresponding number.

1. _____	10. _____	19. _____	28. _____
2. _____	11. _____	20. _____	29. _____
3. _____	12. _____	21. _____	30. _____
4. _____	13. _____	22. _____	
5. _____	14. _____	23. _____	
6. _____	15. _____	24. _____	
7. _____	16. _____	25. _____	
8. _____	17. _____	26. _____	
9. _____	18. _____	27. _____	

Please complete the Evaluation Form (located after the Module 2 Answer Sheet). Thank you.

¶ 10,402 Top Accounting and Auditing Issues for 2024 CPE Course: MODULE 2

Go to **cchcpelink.com/printcpe** to complete your Final Exam online for instant results.

A $120.00 processing fee will be charged for each user submitting Module 2 to **cchcpelink.com/printcpe** for online grading.

Module 2: Answer Sheet

Please answer the questions by indicating the appropriate letter next to the corresponding number.

1. ____	11. ____	21. ____
2. ____	12. ____	22. ____
3. ____	13. ____	23. ____
4. ____	14. ____	24. ____
5. ____	15. ____	25. ____
6. ____	16. ____	26. ____
7. ____	17. ____	27. ____
8. ____	18. ____	28. ____
9. ____	19. ____	29. ____
10. ____	20. ____	30. ____

Please complete the Evaluation Form (located after the Module 2 Answer Sheet). Thank you.

¶ 10,500 Top Accounting and Auditing Issues for 2024 CPE Course: Evaluation Form (10024493-0011)

Please take a few moments to fill out and submit this evaluation to Wolters Kluwer so that we can better provide you with the type of self-study programs you want and need. Thank you.

About This Program

1. Please circle the number that best reflects the extent of your agreement with the following statements:

		Strongly Agree				Strongly Disagree
a.	The Course objectives were met.	5	4	3	2	1
b.	This Course was comprehensive and organized.	5	4	3	2	1
c.	The content was current and technically accurate.	5	4	3	2	1
d.	This Course content was relevant and contributed to achievement of the learning objectives.	5	4	3	2	1
e.	The prerequisite requirements were appropriate.	5	4	3	2	1
f.	This Course was a valuable learning experience.	5	4	3	2	1
g.	The Course completion time was appropriate.	5	4	3	2	1

2. What do you consider to be the strong points of this Course?

3. What improvements can we make to this Course?

THANK YOU FOR TAKING THE TIME TO COMPLETE THIS SURVEY!

CCH® CPELink

Meeting your continuing professional education requirements every year is time consuming enough without spending extra time hunting for relevant courses and keeping track of what you need to take. **CCH® CPELink** gives you your required CPE to maintain your license without giving you a headache. Hundreds of courses over a broad range of topics make it easy to find CPE relevant to your professional development, while the Compliance Manager makes it easy to actively monitor your CPE deadlines and mandatory subject requirements so you don't have to. Take a look at our offerings and feel good about the time you put into your CPE.

- **Webinars.** We offer more than 400 live, online interactive sessions every year, hosted by some of the industry's leading experts.
- **Self-Study.** Learn at your own pace with our online self-study courses. More than 900 courses cover everything from tax and accounting basics to niche topics to help you in your specified field.
- **Print CPE.** This convenient self-study learning is a great way to earn the required CPE credit you need. Download the complimentary course content PDF from CCHCPELink.com/printcpe. When you're ready, return to the website to take the test and earn your CPE.
- **Compliance Manager.** Never miss another CPE deadline! The Compliance Manager includes CPE tracking and compliance monitoring for CPAs in every state (including Puerto Rico) plus many other regulators. Let the Compliance Manager track your CPE so you don't have to.
- **Subscription packages.** Take care of all your CPE needs and save money doing it. View unlimited webinars, save on self-study and webinar hours, or get unlimited CPE for your whole firm. Visit **CCHCPELink.com** for details.

Download your **FREE CPE Course** at CCHCPELink.com/printcpe

Wolters Kluwer