Technology Trends and Hot Topics Impacting the Accounting Profession

THT4/26/V1

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

This Product Is Intended to Serve Solely as an Aid in Continuing Professional Education

- Due to the constantly changing nature of the subject of the materials, this product is not appropriate to serve as the sole resource for any tax and accounting opinion or return position and must be supplemented for such purposes with other current authoritative materials
- The information in this course has been carefully compiled from sources believed to be reliable, but its accuracy is not guaranteed
- In addition, Surgent McCoy CPE, LLC, its authors, and its instructors are not engaged in rendering legal, accounting, or other professional services and will not be held liable for any actions or suits based on this manual or comments made during any presentation
- If legal advice or other expert assistance is required, seek the services of a competent professional

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Overall Learning Objectives

- Identify current and emerging technology trends affecting accounting, auditing, and business operations
- Distinguish among key technologies, including AI, generative AI, agentic AI, RPA, audit data analytics, blockchain, and cloud computing
- Recognize common cybersecurity threats, fraud risks, and IT security vulnerabilities affecting organizations
- Identify common controls and risk management practices used to mitigate technology-related risks
- Explain how accounting and audit professionals are using AI, automation, audit data analytics, and other technologies to improve efficiency and decision-making

Course Overview

- Chapter 1 – Data-Driven Decision-Making
- Chapter 2 – Technology Trends and Risks

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

A Quick Word on Policy vs. Politics

- Many times when discussing accounting, tax and finance policy issues, it can be difficult to divorce the politics from the policy
- Today, when discussing the various issues we will encounter over the next several hours, let's agree to keep our own view of politics out of the application of the policy and focus on doing the very best we can for all our clients
- This goes for religious/faith views as well

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Chapter 1

Data-Driven Decision-Making

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Chapter Learning Objectives

- After completing this chapter, you should be able to:
  - Identify the business drivers of companies today and the need for data-driven decision-making; and
  - Explain the practical steps firms can take to enhance their data-driven capabilities, including tool selection, personnel roles, and cultural change

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

- Global business environment continues to get more and more complex and changes rapidly
- Competition is coming from places where it's least expected; Amazon enters the healthcare space
- Consumer preferences and expectations are changing
- Increased levels of competition due to informed consumers expecting the same level of convenience and service from all entities with which they interact
- Digital disruption continues to reshape entire industries, forcing companies to adapt or risk obsolescence. Consider Blockbuster, Kodak, and others

Data-Driven Decision-Making

- Doesn't take too long for someone's good idea to be imitated with a loss of competitive advantage due to digital connectivity
- Companies are relying on data to help them identify challenges in their operations, take advantage of opportunities, and make timely decisions

EXAMPLE

Amazon is an excellent example of a company that uses data-driven decision-making. Amazon collects enormous amounts of data which continues to increase each year. Amazon makes recommendations to its customers based on click-through rates, open rates, and opt-out rates to decide the products to suggest. They have found that product suggestions drive sales. In addition, Amazon's Echo products, driven by artificial intelligence, are not only widely used by consumers, but a study by Forbes has also identified that Echo users spend 27 percent more on Amazon.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

- Finance and accounting professionals should embrace continuous learning that goes beyond traditional CPE
- New competencies will be needed to succeed in a digital world
- The World Economic Forum's *Future of Jobs Report 2025* estimates that 22 percent of today's jobs will be transformed by technology and other macrotrends by 2030
- AI is increasingly automating routine accounting tasks, allowing professionals to focus more on analysis, judgment, advisory services, and client relationships
- Advances have led to more sophisticated predictive analytics

Data-Driven Decision-Making

- Data provides more valuable and accurate insight than intuition
  - Adam Grant (2021): Gut decision-making often wrong; trust the data and adjust our priors
- Processing at faster speeds and in larger quantities of data contribute to the advancement of AI especially machine learning
- The more data the application has, the better the results
  - Examples – Recommendations by Netflix and Amazon; large language models (LLMs), such as ChatGPT, are trained on large volumes of text and other data to generate responses to user prompts
- Rick Richardson suggests that AI can be developed for common formatted financial statements. Goal would be to highlight anomalies in client statements based on other companies in the industry

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

- Ability to read, transform, and analyze data is becoming key to accounting success alongside technical expertise
- Accounting firms will likely be looking for people with a digital mindset and knowledge of technology who can set up inquiries and tests and interpret results of advanced analytics
- NASBA and AICPA have evolved CPA licensure requirements with the implementation of CPA evolution
- Modifications have validated some of the changes that colleges and universities are already making to curriculum, integrating technology skills that are important now and will become even more so

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 1: True or False

Advances in automation and AI are expected to change the work performed by accounting and finance professionals, increasing the importance of analytical, advisory, and judgment-based skills.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 1: True or False

Advances in automation and AI are expected to change the work performed by accounting and finance professionals, increasing the importance of analytical, advisory, and judgment-based skills.

Answer:

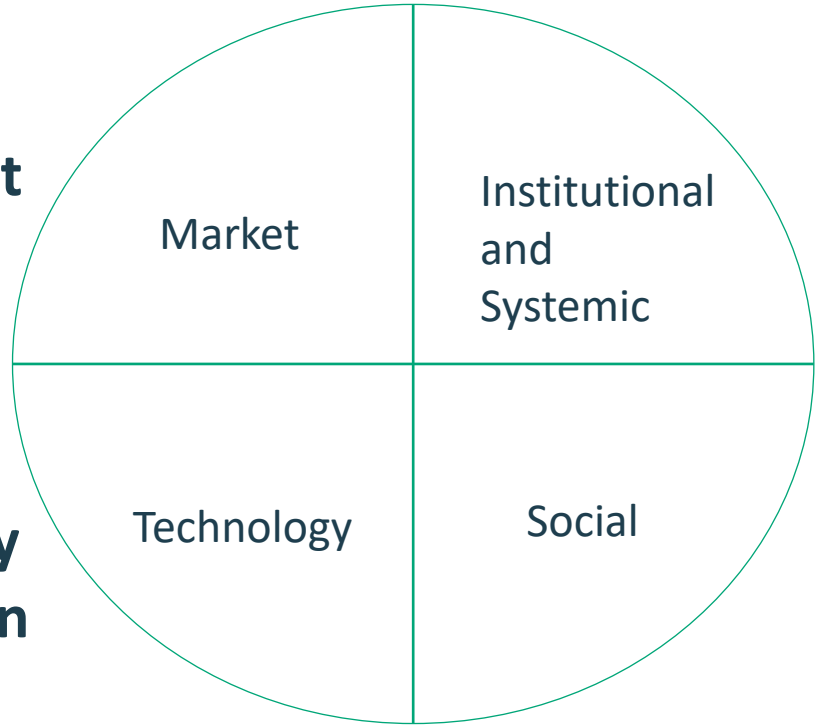
True. AI is increasingly automating routine accounting tasks, allowing professionals to focus more on analysis, judgment, advisory services, and client relationships. As technology continues to evolve, accounting and finance professionals will need to develop new competencies and engage in continuous learning.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Drivers of Change in a Digital World

Consumer Empowerment

Globalization, geopolitics and regulation



Digital Technology Automation

Demographics

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Drivers of Change in a Digital World

Driver	How it shows up in practice
Market	**Consumer empowerment** – Customers are moving from products and services to experiences. They are demanding hyper-personalization moving from ownership to access. They are requiring the same level of responsiveness from all providers as they do from their most responsive providers, raising the bar for all companies
Technology	**Digital technology automation** – Sensors embedded in products send and receive data that provides entities and the finance function with real-time data on their products, services, and financial position. Artificial intelligence, including generative AI and agentic AI, enables entities to engage with customers, optimize operations, research, design, and launch products, and enhance the productivity of their employees The internet, in particular social media, is an area that is transforming the digital world. Its transparency has opened up the field for consumers who have more power to search and compare over a variety of products. Customers can read reviews and compare prices and ratings very quickly

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Drivers of Change in a Digital World

Driver	How it shows up in practice
Institutional and Systemic	**Globalization, geopolitics, supply chain disruption, and regulation** have a significant impact on business operations. Economic influence continues to shift across global markets, requiring companies to monitor international developments and regulatory changes. Countries are investing in AI and data to compete internationally
Social	There are presently **six generations** living in the same economy. More than half of the people live in urban areas. This makes it more challenging for companies to focus and doubly important to understand the patterns of behavior in the way people use technology, consume information, and make purchasing decisions

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

- Companies have increasing amounts of data in their systems that can provide insights to improve processes and performance
- It is not always the right data, and the right data is not always utilized
- Some companies invest in data, analytics, and AI capabilities, while others continue to rely primarily on intuition and experience when making decisions

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

- Industry research[1] highlights key developments shaping the accounting profession, including:
  - Persistent effects of the pandemic
  - Challenges introduced by new technologies
  - Growing importance of advisory services
- The report notes:
  - 67 percent of accounting firms identify as progressive or hybrid, offering significant advisory services
  - Expected advisory growth areas continue to expand beyond compliance services
  - 14 percent expect 70 percent or more of the next 12 months' revenue to come from advisory fees; a further 20 percent expect more than 50 percent

1. Spotlight Reporting's 2025/26 Global Advisory Trends Report

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

- Key areas for potential fee growth identified in the report include:
  - Virtual CFO and advisory work
  - Cash flow forecasting
  - Strategic planning
  - Coaching
  - Ongoing accounting assistance

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

EXAMPLE

On May 15, 2020, after 120 years in business, JC Penney filed for bankruptcy. It was once one of the largest department stores in the country. JC Penney survived the market crash of 1929 and numerous recessions. It successfully entered the digital age and reached its height in 2006. However, by 2010 the latest recession had eroded sales. A real estate firm, Vornado, bought a large stake in the company and removed the current CEO, Myron Ullman replacing him with Ron Johnson who came from Apple. Johnson radically changed the strategy without analyzing the customer base and available data seeking to change the company's market from middle class to more affluent shoppers. Johnson changed the logo, the marketing strategy, pricing model, and brand selection. The change that hit the loyal customer base the most was the elimination of coupons and discounts. The company's sales continued to decline but Johnson did not change course and in 2013 Ullman was brought back to try to reverse the damage. By that time, it was too late. The company was so highly leveraged that it did not have the ability to make the necessary investments in technology to compete with other retailers

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

- Key to digital transformation is to become a data-driven organization using data to drive decision-making
- Concept should be instilled in all employees, not just company leadership
- Companies should leverage data analytics, business intelligence (BI), and AI-enabled tools to understand all aspects of the company's business, including hiring forecasts, supply chain, marketing, and many other finance applications
- Managers and leaders should be challenging decisions and asking what data was used to determine those decisions

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Why Is This Important to Finance and Accounting?

- Finance and accounting are expanding beyond traditional budgeting and forecasting tools
- BI and AI-enabled tools can reveal insights that help improve performance
- Analytics can help determine where resources are generating value
- For example, BI can determine whether a product is yielding less profit than others due to sales effort as opposed to pricing. The insight can be passed along to marketing
- Related tools include predictive analytics, NLP, text analysis, data preparation software, and AI-assisted analytics

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

EXAMPLE

A company invested in BI tools and training for its accounting and finance personnel. Using data analytics, a controller analyzed the company's major products to determine which were yielding the highest margins. He created further queries to determine if the company's marketing campaigns were successful correlating the increase in sales with various campaigns held throughout the year. This helped the CFO and marketing team to determine where money was well spent and where a campaign did not work as well.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Disruptive Technologies

- Finance and accounting professionals should embrace continuous learning beyond traditional education to develop new competencies required for success in a digital world
- The accounting industry is experiencing major disruption from automation, AI, data analytics, and changing client expectations. Routine transactional and compliance activities are increasingly being automated, while professionals are expected to provide more specialized insight, advisory support, and technology-enabled oversight

Disruptive Technologies

- In this evolving landscape, automated and AI-enabled processes are expected to handle many routine tasks under professional oversight, allowing accounting professionals to focus more on specialized advice, insight, technology-enabled oversight, and client relationships
- These shifts are part of five key trends shaping the future of accounting

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Disruptive Technologies

- Initial access to generative AI (GenAI) services like ChatGPT was primarily through specific websites or dedicated mobile apps
- This model is changing as tech companies integrate AI technologies into existing applications instead of providing standalone services
- Microsoft exemplifies this trend, embedding AI in its broad suite of applications with the development of Copilot
- Copilot includes AI-powered features across productivity tools such as Excel, Office, Outlook, and business tools like Power Platform
- Increasingly, AI is embedded directly into business workflows rather than accessed only through standalone applications

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Data-Driven Decision-Making

- Data-driven decision-making provides a systematic, not erratic, approach, helping identify opportunities and challenges
- It allows organizations to quickly and flexibly adapt in volatile markets and dynamic funding environments
- Promotes objective decision-making over subjective, depersonalizing the process for more standardized and consistent decisions
- Reduces the substantial risks associated with reliance solely on intuition for decision-making

Challenges to Data-Driven Decision-Making

- Many organizations have large amounts of data but face challenges with data quality, governance, ownership, and effective use in decision-making
- There is increasing pressure for quick, accurate decisions and timely results
- Adopting a data-driven decision-making approach requires a major shift in organizational culture and mindset
- Employees often prioritize senior leaders' opinions over data-based insights
- Organizations face dilemmas when data-driven recommendations conflict with leaders' directives
- To overcome these challenges, staff at all levels need to improve their analytical skills and regularly use data and analytical tools in their daily work

Barriers to Data-Driven Decision-Making

Barrier	Description
Intuition – A cultural barrier	Although an experienced businessperson's instincts are important, they should be balanced by and informed by data analytics
Data literacy – A cultural barrier	This is a critical element for data-driven decision-making. It is important for the decision-maker to understand and feel confident about the data that goes into the data analysis process and the algorithms used to analyze the data. As organizations adopt AI-enabled tools, data literacy should also include a basic understanding of how AI outputs are generated, reviewed, and evaluated for limitations. The decision-maker needs to be data literate in order to trust the information they have been given by others and understand the data's limitations in decision-making. An important key to data literacy is training and a transparent process
Accountability – A cultural barrier	Decision-makers who are making decisions on intuition should be held accountable for poor decisions. Many individuals in leadership roles may not have sufficient data literacy to fully evaluate data-driven recommendations. An entity needs a process in place to show the steps that need to be followed to make good decisions so issues can be analyzed

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Barriers to Data-Driven Decision-Making

Barrier	Description
Confirmation bias – A cognitive barrier	When someone believes something to be true, they are more likely to remember facts and find support for their beliefs rather than things that refute those beliefs.
Recency bias – A cognitive barrier	People use data points that are recent and do not dig further. Important patterns are developed over the long term and to give recent information heavier weight is a critical error. Ask the question: why is the most recent data more important than historical data? It may be but this should be justified.
Illusion of validity – A cognitive barrier	It is easy to see patterns that are not actually there. Sometimes people's brains try to make connections that are not present. An example could be reviewing a document that you just wrote. The writer knows what they meant and does not see mistakes. The brain automatically fills in the gaps.

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Cognitive Barriers to Data-Driven Decision-Making

Barrier	Description
Rigid mental models – A cognitive barrier	Mental models are constructed from patterns. For example, if an entity has an established pattern for marketing that is tried and true, it will work for a while. But if the entity sticks to that mental model long enough, new variables will be introduced into the system, and the validity of the model will suffer. It is important to keep models flexible and adaptable. A critical aspect of good modeling is to revise models since they become stale over time, including data models and AI-assisted analytical models.

Solving Barriers to Data-Driven Decision-Making

Approach to handling barrier	Description
Incentives and accountability	Performance needs to be measured against quantitative measures. Feedback loops are important as is cross-functional communication so that all members of a team can provide feedback and share successes and failures. If the culture does not penalize failures, it is more likely that employees will share feedback. Accountability for performance against objective measurements is critical in a data-driven culture
Data-based proof approach	Data-based proof is used to demonstrate that the data and the process an analyst is using are appropriate for the decision to be made. It is important that data is clean, reliable, and appropriately governed so it can be trusted. It is also important to map the data out so that the analyst can evaluate the tools and technology available to use for making the decision. The process of making the decision needs to be relevant to the problem that the analyst is trying to solve. When AI-enabled tools are used, the process should also include review of the inputs, assumptions, and outputs

Solving Barriers to Data-Driven Decision-Making

Approach to handling barrier	Description
Transparency	Transparency helps to protect against confirmation and recency bias because more people are seeing the data. Responsibilities for the analysis should be made clear, and outcomes of the analysis should be disseminated
Abilities	It is important to either provide people with the right training or, alternatively, for a company to hire people with the relevant skill sets. Continuing education should be a priority. Companies should be aware that there will be a wide talent gap when first undertaking to become a data-driven organization. This includes gaps in data literacy, analytics, and AI literacy
Actions tied to outcomes	Results should be able to be traced back to the needs of the company

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 2: True or False

a. **The barriers to data-driven decision-making can be categorized as cultural and cognitive. Probably the hardest to overcome is intuition.**

b. **Which do you think is the hardest to overcome**
   - **Intuition;**
   - **Data literacy;**
   - **Accountability;**
   - **Confirmation bias;**
   - **Recency bias;**
   - **Illusion of validity; or**
   - **Mental model?**

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 2: True or False

a. The barriers to data-driven decision-making can be categorized as cultural and cognitive. Probably the hardest to overcome is intuition.

Answer: True.

b. Which do you think is the hardest to overcome

- **Intuition;**
- **Data literacy;**
- **Accountability;**
- **Confirmation bias;**
- **Recency bias;**
- **Illusion of validity; or**
- **Mental model?**

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Steps To Become a More Data-Driven Entity

1. **Decide** what to measure
   - Do not measure trivial things because the data is easy to collect
   - Keep the questions that the entity wants to answer in mind. It is expensive to collect data
   - If there is an easier way to obtain the data, for example by purchase, then use the alternative method
   - Ask the question: How precise does the answer need to be?
   - Consider whether the data will be used in AI-enabled tools, as this may require additional attention to data quality, governance, and relevance

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Steps To Become a More Data-Driven Entity (Cont.)

2. **Choose** the correct BI tools
   - Excel has come a long way, but it will not be robust enough for large data sets or complex analysis
   - For big data analysis, use sophisticated tools that:
     - Provide robust data ingestion, integration, and preparation features;
     - Consume data through file uploads, database querying, and application connections;
     - Allow for modeling, blending, and discovery of data;
     - Create reports and visualizations with business utility;
     - Create and deploy internal analytics applications; and
     - Provide AI-enabled features, such as natural language queries, automated insights, or anomaly detection, where appropriate

Steps To Become a More Data-Driven Entity (Cont.)

2. **Choose** the correct BI tools

- G2, a clearinghouse of information related to reviews of BI, regularly analyzes reviews and provides up-to-date insights. Below are some of the highest-performing products based on user satisfaction and performance scores[1]:

Product	Reviewer Satisfaction Score (1-100)	G2 Score (1-100)
Amazon QuickSight	87	93
Tableau	96	91
Canva	100	90
Looker	98	85
Google Earth Engine	77	81
Microsoft Power BI Embedded	68	74
GoodData	89	74
Looker Studio	60	73
AgencyAnalytics	93	73
Salesforce Maps	79	73
Domo	74	72
Sigma	86	71
IBM Cognos Analytics	58	69

1. Data retrieved from G2's Business Intelligence Grid® Report for Business, Spring 2025 (https://www.g2.com/categories/business-intelligence/resources)

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Steps To Become a More Data-Driven Entity (Cont.)

3. **Identify** staff with the aptitude and interest to become proficient in analyzing and presenting data. This may include developing skills in analytics, data visualization, and AI literacy. Where necessary, recruit people with experience to supplement the existing team
4. **Address the issue of decentralized data** – Many systems are siloed making data analysis more challenging. Sometimes it takes more effort to compile and prepare the data than analyze it
   - Some entities may find full system integration too expensive but should look for ways to automate processes and analyze critical data while maintaining appropriate governance, access controls, and data integrity
   - When selecting a new system, the ability to fully integrate with existing systems should be an important consideration

Steps To Become a More Data-Driven Entity (Cont.)

5. **Data Security and Data Integrity**

- **Data security** – Keeping data safe from unauthorized users. It includes:
  - Hardware solutions such as firewalls
  - Software solutions such as multifactor authentication and encryption
  - It is critical in preventing cyber-attacks
  - Data security is the fundamental general computer control
- **Data integrity** builds on data security to help to ensure that the data used in analysis and for other purposes is valid, accurate, and consistent
- Data integrity can also be a process
  - Describes measures used to ensure validity and accuracy of data or a set of data contained in a database or some other construct
  - Error checking and validation methods are considered data integrity processes
  - This is especially important when data is used in dashboards, automated workflows, or AI-enabled tools

Steps To Become a More Data-Driven Entity (Cont.)

5. Data Integrity

- If data lacks integrity, then it is useless to the analyst since the insights gained from analysis are then suspect
- As data travels through a system, it must remain intact. Data can be damaged:
  - In transit from a computer to a storage device or over a network
  - Hardware failures in storage devices or the computer itself can occur
  - Software or security applications can be misconfigured resulting in damaged data
  - A deliberate breach can occur where a person or software compromises a system and changes data. For example, malware (ransomware) encrypts data and holds it hostage for payment. Alternatively, a threat actor may breach the system and make changes

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Steps To Become a More Data-Driven Entity (Cont.)

5. Data Integrity

- Data integrity has several important aspects:
  - Data should have the time, date, and identity of who recorded it
  - Data should be in a standardized format and easy to read
  - Data should be timely. Any time there is a delay in recording data there is an opportunity for loss
  - Good data is maintained in its original format
  - It should be secured and backed up
  - Data should be free of errors
- The system should have:
  - Controls to validate the input and the data itself;
  - Controls to create backups;
  - Access controls; and
  - An audit trail

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Steps To Become a More Data-Driven Entity (Cont.)

6. Create a culture shift

- As noted earlier a culture shift will be necessary to create a successfully data-driven organization. Leadership must be fully on board and “walk the talk.” Addressing the cultural and cognitive issues outlined above can help instill a digital mindset in employees
- Keys to effective implementation:
  - Communication;
  - Training;
  - Enforcing new policies and procedures; and
  - Responsible use of data and AI-enabled tools

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Chapter 2

Technology Trends and Risks

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Chapter Learning Objectives

- After completing this chapter, you should be able to:
  - Identify and discuss the top 10 technology trends and risks;
  - Understand the methodology for using audit data analytics;
  - Identify the most common cyber fraud schemes used today; and
  - Identify ways to help prevent cyber fraud

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top 10 Technology Trends

1. Artificial intelligence, including generative AI and agentic AI
2. Cloud computing
3. Robotic process automation
4. Advanced data analytics
5. Integration of accounting and operations systems
6. Outsourcing and offshoring the accounting function
7. Accounting and finance professionals need new skill sets
8. Focus on transparency, objectivity, and validity – blockchain
9. Remote and hybrid accounting workflows
10. Changes in professional literature and internal control guidance

Artificial Intelligence (AI)

- AI, including generative AI and agentic AI, is growing in prevalence and in scope
- AI can extract key information, generate content, automate tasks, and detect patterns or anomalies at scale
- This trend has the potential to change how finance, accounting, and auditing professionals do their jobs
- Algorithms are being written that can evaluate large quantities of data and identify anomalies and risks, as well as find opportunities to enhance profitability
- If AI provides the user with an answer, they may want to understand how the program came to that determination
  - Not always possible with LLMs

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Artificial Intelligence (AI)

- AI uses logic, rules, statistical models, and learning algorithms to form the instructions that are the basis of the algorithms
- The most widely used application of AI is machine learning, which relies on the application learning over time rather than on rules-based instructions
- The algorithms themselves create models that process large data sets that predict outcomes and infer information from the data (e.g., Large language models such as ChatGPT, Claude, or Gemini)
  - The machine learns and adjusts the algorithm over time
- Common applications that people use every day are email spam filters, spell check, predictive text, and voice recognition systems
- There are several different types of machine learning that are used to solve two types of problems: regression and classification
- Regression problems are solved by prediction, and classification problems involve classifying input, such as whether a transaction is an anomaly or not

Artificial Intelligence (AI)

- Machine learning may be supervised
- The system is provided with many data points, and each data point is tied to an expected outcome. The machine begins to develop how data relates to the expected outcome. As the machine is trained it provides a more useful answer

EXAMPLE

An AI application was developed to assess whether customers were credit worthy. To train the system, thousands of transactions with numerous data points about the potential borrowers were provided for analysis from past loan applications. The data was historic, enabling the machine to know which borrowers were credit worthy, and which ones defaulted on the loan. The system was then able to develop its own set of rules to determine when a future applicant should be approved.

Artificial Intelligence (AI)

- Machine learning can also be unsupervised
- An algorithm is developed where the system is looking for similarities. Companies like Amazon and Netflix use this form of AI to make recommendations
- The system looks for similar customers, and their purchases inform the recommendations for another customer
- In the audit space, unsupervised machine learning could be used to identify transactions that are not typical that may be the result of errors or fraud

Artificial Intelligence (AI) – LLMs

- Large language models (LLMs) have the ability to generate text, tables, and responses by "learning" from large quantities of data to identify patterns and trends
  - Examples include ChatGPT, Claude, Gemini, Copilot, and other AI assistants embedded in business applications
- GenAI tools are trained on large volumes of text and code to generate text, tables, summaries, and basic code
- Designed to produce human-like responses
  - Answers improve as you refine your prompt and follow-up with the AI
- Remember:
  - Better prompts = better answers
  - Bad information in = bad information out

Artificial Intelligence (AI) – LLMs

- LLMs impact in accounting, auditing and finance
  - Clients may use it like medical patients WebMD – Be prepared to respond
  - Can summarize new ASUs, SASs, tax laws, and other authoritative guidance
    - Warning: It's not always correct – It has shown to create authoritative sounding guidance and code sections that do not exist
  - Replace staff writing tasks – Still requires technical review
  - Client data – Understand your organization's policies before entering sensitive information into AI tools. Data handling, retention, and training practices vary by provider and deployment model
- Each version gets progressively better by degrees of magnitude
  - AI capabilities continue to evolve rapidly, with significant improvements occurring over months rather than years

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Artificial Intelligence (AI) – LLMs

- Since its debut in November 2022, generative artificial intelligence (GenAI) such as ChatGPT has been utilized in many ways among tech-savvy accountants
- GenAI tools are utilized for drafting emails, analyzing spreadsheets, summarizing tax laws, researching business plans, generating code, and aiding in practicing difficult client conversations
- Effective use of GenAI tools depends on crafting clear, specific prompts, providing appropriate context, and verifying outputs before relying on them
- Poorly constructed prompts can result in disappointing outputs, factual errors, or flawed code, masking the true potential of the technology

Artificial Intelligence (AI) – LLMs

- Conversely, well-crafted prompts unlock the full capabilities of large language models, helping finance professionals to innovate and speed up their work
- A recent study highlighted significant improvements in the GPT model's performance on an unofficial practice CPA Exam, demonstrating the impact of effective prompt engineering
- Researchers used prompt engineering techniques to enhance the GPT model's performance from failing to passing on an unofficial practice exam. Improving prompt quality doesn't require technical expertise or programming skills, but rather clear, specific instructions, as well as creative experimentation by the user

Agentic AI and Autonomous Tools

- Key capabilities:
  - AI agents that plan, execute, and adapt across tasks
  - Tools that operate autonomously using APIs and multiple apps
  - Embedded copilots in Microsoft Excel
  - Chatbots that trigger workflows and retrieve real-time data
- Examples:
  - Microsoft Copilot agents or Claude agents
  - AI copilots integrated in business platforms
  - Automation-triggering chatbots
  - AI-enabled workflows that monitor transactions, draft analyses, prepare reconciliations, or route exceptions for review
- Opportunities and risks:
  - Efficiency gains through intelligent task automation
  - New concerns: privacy, bias, auditability, governance, access rights, and accountability
  - Professionals must understand both capabilities and ethical limitations when applying agentic AI in financial and client-facing contexts

Cloud Computing

- According to a BlackLine survey, nearly 40 percent of CFOs worldwide doubt the accuracy of their organization's financial data
- The survey included over 1,300 C-suite and senior finance and accounting professionals across seven markets: the United States, Canada, the United Kingdom, France, Germany, Australia, and Singapore
- Findings show 37 percent of CFOs and approximately 50 percent of senior finance and accounting professionals lack full trust in their financial data

Cloud Computing

- Owen Ryan, co-CEO of BlackLine, stressed the critical role of data trustworthiness for effective decision-making across the business ecosystem, especially amid unpredictable external events. The survey also revealed significant concern among respondents about external threats: 78 percent fear a global financial crisis, 76 percent are concerned about cybersecurity issues, and 73 percent worry about the impact of disruptive technologies on their business
- The survey also highlighted persistent concerns about financial visibility, with 98 percent of respondents lacking full confidence in their organization's cash flow visibility for the second consecutive year. Additionally, 37 percent recognize that real-time cash flow insight is crucial for effectively managing unexpected market changes

Cloud Computing

- Cloud-based accounting solutions are gaining in popularity. Companies are currently producing more and more data in the form of:
  - Transactional data;
  - Data collected from the IoT (internet of things), which could be data from appliances, consumer wearables, temperature-checking devices, devices such as Alexa that track activities by the user, and more; and
  - Data on customers collected from questions asked by point of service devices
- Many IT systems are not equipped to handle the volume of data

Cloud Computing

- Cloud computing is essentially outsourcing the processing of an entity's data to a network of remote servers hosted on the internet
- Cloud computing is scalable so both small and large entities can use it
- Companies would no longer need to buy and maintain expensive IT systems
- Robust processing power is a significant benefit and is very important when it comes to performing advanced data analytics and using AI
- Many platforms now include built-in AI tools like machine learning, anomaly detection, and NLP to help finance teams analyze structured and unstructured data more efficiently
- As cloud adoption expands, organizations must also consider vendor risk, access controls, data governance, and security over cloud-based financial information

Robotic Process Automation

- Robotic process automation (RPA) mimics tasks that are performed by humans and automates them
- Used to handle high volume tasks that are repeatable such as making calculations or recording transactions
  - Can include replicating mouse clicks, keystrokes, and ETL data tasks
- RPA is more consistent and accurate and can handle these tasks more quickly than a human can

EXAMPLE

A programmer was developing an RPA application. It was written to:

- Download a file;
- Take certain data from the file;
- Transfer that data to another file; and
- Save the document.

This set of repetitive tasks, which was previously performed by an employee, did not involve decision-making. The RPA application saved the company 400 person hours a year and accuracy was improved.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 3: True or False

Robotic process automation (RPA) is an application that mimics the tasks of humans. A good example would be a telephone answering system.

Discussion Question – True or False

Question 3: True or False

Robotic process automation (RPA) is an application that mimics the tasks of humans. A good example would be a telephone answering system.

Answer:

False. RPA automates highly repetitive tasks that are processed in large volume. An example would be processing credit card limit increases. The bot can examine customer accounts and based on predetermined criteria, approve or deny increases.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Advanced Data Analytics

- Companies and auditors already use data analytics
- Explosion of data coming from the IoT, social media, mobile computing, cloud platforms, and AI-enabled systems
- Use of more sophisticated analytics can give companies and auditors more insight into the business drivers of the company
- They are a tool to identify unusual relationships that need further scrutiny and make predictions about what will happen

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Advanced Data Analytics

- ***Descriptive analytics*** – Provides insights into the past and helps the analyst determine what happened
- ***Diagnostic analytics*** – Involves the examination of data to answer why something may have happened
- ***Predictive analytics*** – Technique used to predict the future to forecast what will happen. Auditors may use these techniques to predict balances in substantive analytical procedures
- ***Prescriptive analytics*** – Technique that builds on predictive analytics and answers the question, "How do we make it happen?"

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Descriptive Data Analytics

EXAMPLE

An auditor was evaluating accounts receivable. She was able to identify which of the balances at year end were cleared by payment and which were written off or cleared by credit memo. She was also able to look at the customers from the prior year in hindsight and determine if the allowance was adequate based on amounts collected in the current year. She was able to obtain information about the collection process by identifying the customers with past due balances, the date of follow up, and other remarks made by those responsible for following up on past due balances. In prior years this would have been a long laborious process, but analytic software enabled the insight into the valuation methods and helped her to understand how well the client developed the estimate for the allowance for credit losses.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Diagnostic Data Analytics

EXAMPLE

An auditor noted that sales were down during the year. He was curious because the number of sales in units increased and there were no price reductions on the price list. By using diagnostic analysis, he was able to drill further down into the sales balances. Using this technique, he was able to prepare a graph that showed that the decrease in sales started in the month of April. He made inquiries as to whether there were any changes in personnel in the March/April timeframe. He learned that a new sales manager had been hired in February. Shortly thereafter the manager tired of approving requests for discount and instituted a policy change that allowed salespeople to give discounts up to 15 percent without approval.

The auditor went back and performed a further analytic to determine if the percentage discounts on sales of product increased and determined that this was the anomaly in sales. This insight was added to the substantive analytical procedure. In addition, the auditor was able to let the sales manager and the CFO understand the ramifications of the policy change

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Predictive Data Analytics

EXAMPLE

An operations manager of a chain of stores that sell ice cream wanted to find a way to fine tune her estimate of demand so that she could ensure that the product was delivered to the stores when needed and could avoid ordering product before it was needed. She had data on sales per day from the past several years. She observed that outside temperatures were correlated with sales. Other factors that appeared to play a role were school holidays. She used this data as well as the predicted weather forecast for the upcoming period to estimate demand

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Prescriptive Data Analytics

EXAMPLE

A production manager used prescriptive analytics to guide predictions into action steps. The system provided him with an alert that a material needed to manufacture an input to a product was low and more was needed to complete a new order. The prescriptive analytic evaluates the inputs needed and orders the product needed to fulfil the order

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Types of Analytical Procedures on the Audit

- Analytical procedures are an offshoot of audit data analytics
- Analytical procedures are a natural extension of the auditor's understanding of the client's business
  - Preliminary – Required (AU-C 315)
    - Assist in planning the nature, timing, and extent of further procedures
  - Substantive – Auditor may find these beneficial (AU-C 520)
    - Purpose is to obtain evidence, sometimes with other procedures, to identify misstatements and reduce audit risk
  - Final – Required (AU-C 330)
    - Assist the auditor in assessing conclusions reached and evaluating the overall financial statement presentation

Audit Analytical Procedures

- SAS No. 145 requires firms to understand how technology impacts an entity's financial statement preparation, influencing tailored audit planning and procedures
- If a client adopts new technology, firms must adjust and not merely replicate old audit processes, which might be obsolete
- Firms need a deep understanding of new technologies to assess their impact on client workflows and to modify audit procedures accordingly

Audit Analytical Procedures

- SAS No. 145 encourages auditors to use technology for data analysis and to innovate their auditing methods
- Incorporating technology and data analytics in auditing helps overcome the constraints of traditional sampling, allowing for a full dataset analysis to identify anomalies, trends, and risks for a more comprehensive data understanding

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Integration of Accounting and Operations Systems

- More companies are upgrading their basic systems, like QuickBooks with integrated accounting systems
- When data is housed in different systems that are unable to communicate directly with each other, the company runs the risk of errors and is not able to perform the types of analytics that would be possible with an integrated system
- Larger entities may have the ability to afford to run Enterprise Resource Planning (ERP) systems
- An ERP system incorporates data from several different business processes into a comprehensive information system
- This is increasingly important as organizations seek clean, connected data for dashboards, automation, and AI-enabled analysis

Integration of Accounting and Operations Systems

- Financial and operational data that is stored in ERP data warehouses gives the entity a way to run advanced analytics and it can incorporate data of multiple companies
- ERP streamlines processing because the system components interface
- For example, a customer service representative can be given access to ordering information which includes shipping details. If there are delays in shipping or more information is needed the customer service employee can inform the customer. An HR employee can be given access to some payroll functions

Integration of Accounting and Operations Systems

- Smaller entities that cannot afford an ERP system may decide to choose an integrated accounting system as a stepping-stone as they grow
- The integrated accounting system incorporates functions specific to accounting
- An ERP system has a lot more components, such as human resources, inventory management, sales and distribution, and supplier and purchase order management, as well as the general ledger, accounts receivable and payable, and other finance applications (financial management module)
- Although the integrated accounting system has aspects of financial as well as cost accounting such as general ledger, journal entries, accounts payable, accounts receivable, inventory, and fixed asset accounting, it does not have the capabilities of interaction that an ERP financial management module has
- When evaluating these systems, entities should also consider whether the platform supports secure integrations, APIs, and reliable data flows between accounting, operational, and reporting tools

Outsourcing Accounting Functions

- Some businesses are outsourcing their entire accounting functions to third parties so they can concentrate on operations
- Business Process Outsourcing (BPO) continues to grow steadily, driven in part by demand for finance and accounting services enhanced with AI and automation
- BPO providers have economies of scale and typically operate in low-cost countries. By outsourcing the accounting function an entity does not have to invest in the technology that continues to improve each year
- Outsourcing has its drawbacks. Data breaches, quality issues, and perhaps being in a country with an unstable government can have a big impact on a company
- Quality assurance and strong internal control over financial reporting (ICFR) should be top priorities when outsourcing accounting – evaluate providers' cybersecurity, staffing, and certifications (e.g., SOC 1/2, ISO 27001) to avoid downstream risks

Accounting and Finance Professionals Need Different Skill Sets

- The biggest challenge that a company's accounting firm will face going forward is that employees who completed their formal education several years ago may lack the up-to-date technical and analytical skill sets needed in today's digital environment
- A survey by Robert Half asked approximately 1,100 CFOs about their needs and challenges finding qualified personnel
  - 37 percent of CFOs said that business analytics skills were mandatory for everyone
  - 49 percent said that they were mandatory for certain positions
  - 12 percent said they were nice to have but not mandatory
  - 2 percent said they were rarely needed or not needed at all

Accounting and Finance Professionals Need Different Skill Sets

- CFOs rated the following attributes as the hardest to find in accounting and finance job candidates

Technology experience or aptitude	32%
Functional job skills	21%
Leadership abilities	18%
Soft skills such as interpersonal and communication skills	16%
Organizational fit	12%

- According to another Robert Half survey focused on public accounting, public accounting firms hiring managers are having similar challenges

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Accounting and Finance Professionals Need Different Skill Sets

- The hiring market is competitive
- Many of the candidates available do not have the skills that will be needed in the future. The primary skill that is lacking is technology skills
- Other important skills include critical thinking, communication, and emotional intelligence
- More and more companies are providing training and other opportunities for their personnel to acquire or enhance their business analytics skills
- Public accounting firms may find it is easier to identify current employees with aptitude and help them improve in the areas needed

Accounting and Finance Professionals Need Different Skill Sets

- As a client's IT system becomes more integrated and the technologies the client is employing become more sophisticated, the composition of the audit team may need to change
- When choosing audit team members to understand and test IT controls it is also important that they understand the system development lifecycle for emerging technologies
- Traditional audit team members may not have deep expertise in IT so it may be difficult for them to develop an adequate understanding of the design and implementation of these controls
- If information is only available in electronic form, which is a trend, controls will need to be tested
- The audit team should determine whether a person with specialized skills is needed to perform this work

Discussion Question

Question 4: Multiple Choice

Whether you are in public accounting or industry, do you feel like your entity is equipped to move into the use of using/auditing new technologies?

A. Yes, my firm/entity has dedicated people that have sufficient expertise that we don't see any needs arising

B. No, my firm/entity does not have the expertise in house and is already having trouble finding people to fill these roles

C. We haven't really started thinking about this yet

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question

Question 4: Multiple Choice

Whether you are in public accounting or industry, do you feel like your entity is equipped to move into the use of using/auditing new technologies?

A. **Yes, my firm/entity has dedicated people that have sufficient expertise that we don't see any needs arising**

B. **No, my firm/entity does not have the expertise in house and is already having trouble finding people to fill these roles**

C. **We haven't really started thinking about this yet**

Answer: There is no specific answer to this question

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Focus on Transparency, Objectivity, and Validity – Blockchain

- Blockchain promotes the notion of transparency, objectivity, and validity
- Blockchain originated in 2008 but only emerged as an important force for commerce when bitcoin launched in 2009
- Satoshi Nakamoto wrote a white paper titled *Bitcoin: A Peer-to-Peer Cash System* and described a system for electronic transactions that did not rely on trust
- A reference to Chancellor Alistair Darling and the second bailout of banks was embedded in the first bitcoin transaction
- Blockchain presents a solution to the problem: “How does a party to a transaction know if something is real or not?”

Focus on Transparency, Objectivity, and Validity – Blockchain

- Consider dollar bills. They are identified with serial numbers
- To unequivocally determine if a dollar bill is valid, the party receiving it would need to consult with a central authority that maintains the listing of serial numbers
- When there is a centralized party, the power to make changes that are unauthorized is centralized
- Blockchain technology is designed to be highly resistant to alteration and relies on distributed consensus mechanisms
- Since the digital information is distributed and not maintained in a single location, it cannot be easily altered by others

Focus on Transparency, Objectivity, and Validity – Blockchain

- Since anyone can join public blockchains if they have the specialized hardware, there are multiple eyes on every transaction
- Information is duplicated thousands of times across a network of computers, and is constantly reconciled into the database, stored in multiple locations, and updated instantly; it is nearly impossible to hack
- The “block” is a record of a new transaction and when it has been verified it is added to the chain
- There is no centralized processing entity (middleman) needed for these transactions who would likely take a percentage of the transaction as a fee

Focus on Transparency, Objectivity, and Validity – Blockchain

- Most large transactions are processed now by financial institutions. When a request to transfer money is made by a customer to transfer funds in a transaction, the custodial bank has to coordinate, synchronize, and message with the other bank to ensure that the transaction happens the way it was instructed. There are two disparate databases
- With blockchain there would be one ledger of transaction entries to which both parties have access, streamlining the process
- The blockchain then is a distributed ledger which houses the details for every transaction ever processed on the chain
- The validity and authenticity are protected by cryptography (digital signatures)

Focus on Transparency, Objectivity, and Validity – Blockchain

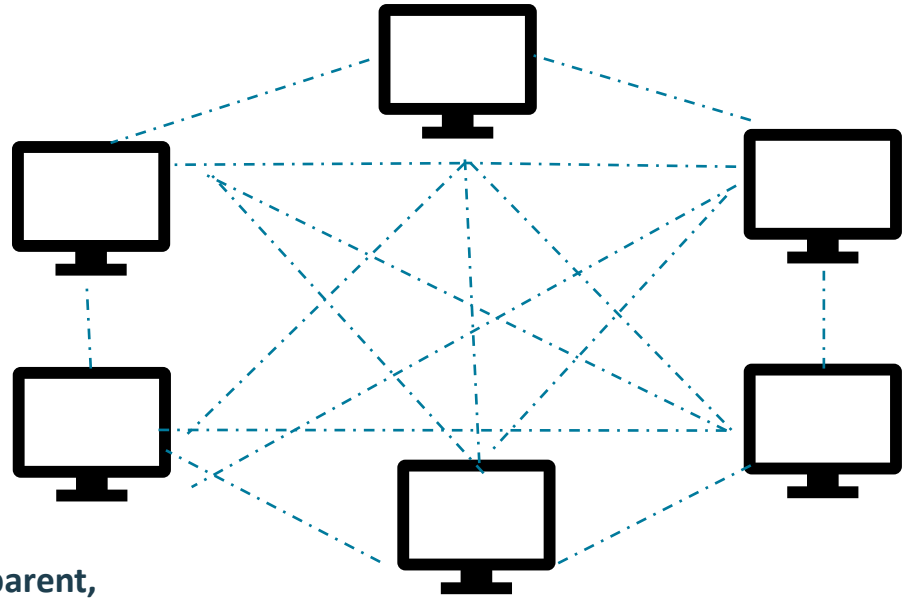
- A blockchain serves as an open ledger, independently verified by two parties, that cannot be altered
- It could be used as a source of verification for reported transactions
- Blockchain technology may provide auditors with additional sources of audit evidence and may reduce the need for certain traditional confirmation procedures in some circumstances
  - Auditing standards would need to adapt to this possibility
- Enhance audit coverage in a major way
- Since blockchain is almost “real-time,” a continuous audit could be performed

Focus on Transparency, Objectivity, and Validity – Blockchain

- Blockchain has risks – In 2022, threat actors stole approximately $3.8 billion in digital currencies according to a report by Chainanalysis
- The issue typically is not with the blockchain per se, but with the currency wallets and computers of the parties to the blockchain
- Illustrates that if blockchain is to be universally accepted the underlying environment needs to be secure. This would shift the audit processes away from substantive testing and push the testing toward the entity's IT controls
  - DOJ has been able to recover stolen crypto funds; many transactions now traceable
- GAAS requires auditors to understand the risks to the financial statements resulting from information technology where it is significant. Auditors are required to test internal controls when information is only available in electronic form and is complex as it would be in the use of blockchain

Blockchain – Simplified Illustration 1/2

Transactions are secured by digital signatures and cryptography



Computers are connected on the internet. Any one computer can send to or receive from another

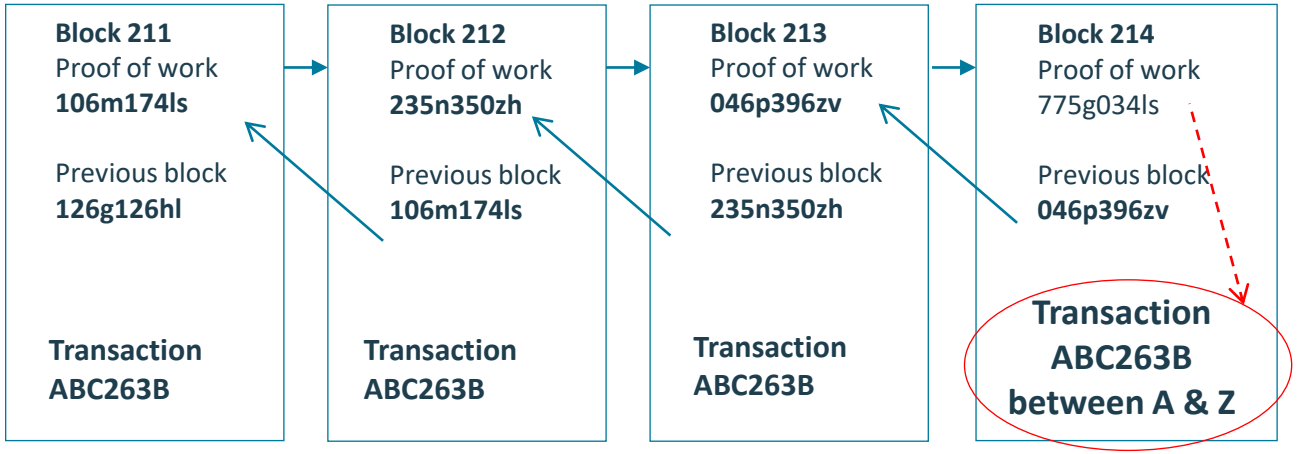
There is no middle-man or central clearing house. The transfer is peer to peer

Transactions cannot be modified. They are transparent, searchable and can be seen by all participants

Transactions are in chronological order (block number) and it gets larger as more transactions are made

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Blockchain – Simplified Illustration 2/2



The blockchain nodes (miners) execute functions to confirm and authorize the transaction. This is referred to as proof of work. Then the transaction is recorded.

Company A wants to execute a transaction with Company Z. In order for this to happen the nodes on the network (miner) will need to authenticate Company A's transaction. The miners use their ledger (the blockchain) to determine if Company A has the bitcoin to transfer to Company Z. The blockchain contains all the records and so the miner can add up all the transactions that Company A has ever made (both as recipient and as funder). Once the amount is validated the miners add the verified transaction to the blockchain and then add it to the previous block which was verified as a part of another transaction. Validation occurs using key cryptography.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 5: True or False

Two significant characteristics of blockchain which enhance people's trust in using it are that it requires a central clearing house, and it is distributed.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 5: True or False

Two significant characteristics of blockchain which enhance people's trust in using it are that it requires a central clearing house, and it is distributed.

Answer:

False. The characteristics that make people tend to trust blockchain are that it is distributed and that it is immutable (can't be changed).

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Remote and Hybrid Accountants

- Widespread adoption of cloud computing and electronic documentation has enabled more accountants to work remotely or in hybrid environments
- Standard practices now include:
  - Cloud audit platforms
  - Secure document portals
  - Remote collaboration tools
  - AI-enhanced document review and confirmation systems
- Benefits: efficient, real-time, secure workflows
- Key risks: access, identity, and digital evidence control
- Same level of professional skepticism and data governance required as traditional engagements

Changes in Professional Literature

- As entities and their accountants embrace technology, technical literature will need to change as well
- New business models have a significant impact on accounting and auditing. FASB and GASB will continue to evaluate accounting literature
- The Committee of Sponsoring Organization's (COSO) framework is the most widely used internal control framework in the United States
- The primary reason for the extensive updates to the framework in 2013 was to include robust considerations about controls over information technology
- Where these controls applied primarily to larger more sophisticated companies in 2013, today they are more widely applicable, and some are relevant to all entities

COSO Framework

- The most prevalent framework used for internal control over financial reporting is the COSO framework
- There are 5 elements of internal control identified in the framework:
  - Control environment;
  - Risk assessment process;
  - Control activities;
  - Information and communication; and
  - Monitoring

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Risk Assessment

Element 2 – Risk Assessment

- Any change in a client's business processes and financial reporting system, no matter how beneficial, brings an element of risk. This is especially true in information technology (IT)

Risk Assessment

- Regarding the risk assessment element as it addresses IT, management should consider the following:
  - The entity identifies risks to achieving its objectives and analyzes risks to determine how the risks should be managed
  - Mechanisms are in place to identify risks potentially affecting the achievement of the entity's objectives, including:
    - Changes in operating, economic, and regulatory environments;
    - Participating in new programs or activities;
    - Offering new services;
    - Communication at various levels of management;
    - Application processes; and
    - **IT infrastructure and processes**

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Risk Assessment

- Using a Risk and Controls Matrix to Map Risks to Control Activities

EXAMPLE

Elite Picture Frame Company (EPF) is a manufacturer of moderately priced picture frames. In connection with its risk assessment process, the company has developed a decision-support matrix covering financial reporting assertions and objectives, identified risks, and control activities. The matrix addresses areas such as regulatory matters, financial statement preparation, closing and consolidation processes, estimates and reserves, accruals, and general ledger procedures. Each control is addressed in enough detail to permit evaluation as to whether it could be effective in reducing the relevant risk to an acceptable level. Management also evaluates the mix of different types of controls (such as prevention vs. detection and automated vs. manual).

Risk and Controls Matrix (Example 1/2)

Flow of the Ordering Process

Purchasing Department

1. Initiate Purchase Order
2. Update Vendor Master File
3. Update Price Master File
4. Send to AP System

AP System

1. Perform Edit and Validation
2. Update Vendor Master File
3. Update Price Master File
4. Return to Purchasing Department

Purchasing Department

1. Generate Purchase Order
2. Send to Buyer

Buyer

1. Approve Purchase Order
2. Send to Accounting Department

Flow of the Invoice Processing

Accounting Department

1. Receive Invoice from Vendor
2. Input Invoice
3. Update AP Ledger
4. Receive Approved Purchase Order from Buyer
5. Receive Goods Received Document from Receiving Department
6. Match Invoice / Purchase Order / Goods Received Document
7. Record Invoice
8. Update General Ledger

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Risk and Controls Matrix (Example 2/2)

Using a Risk and Controls Matrix

Control	Financial Risk	F/S Asser-tions	Control Level	Frequency	Description	Manual/ Automated	Prevent/ Detect	IT Objective
1	Inaccurate Orders	V	Transaction	"N" Times Daily	IT sys runs validity checks, then updates master and transaction files	Automated	Prevent	A, V
2	Order from Unapproved Vendor	E/O	Transaction	"N" Times Daily	IT sys blocks POs with master file items (e.g. vendor) not matching master file, sends to PO exception report	Automated	Prevent	A, V
3	Inaccurate Order Prices	V	Transaction	"N" Times Daily	Purch mgr must approve pricing different from master file, else IT sys cancels PO	Manual	Prevent	A, V
4	Inaccurate or Invalid Orders	V, E/O	Transaction	"N" Times Daily	Each PO must be approved by buyer, who does various validity checks	Manual	Prevent	A, V
5	Inaccurate or Invalid Invoice Processing	V, E/O, R&O	Transaction	"N" Times Daily	IT sys matches Invoice/PO/ReceivingDoc. If no match, sends to Matching Exception Report	Automated	Prevent	A, V

Assertions: E/O=Existence/Occurrence, C=Completeness, V=Valuation/Allocation, R&O=Rights and Obligations

IT Objectives: C=Completeness, A=Accuracy, V=Validity

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Risk Assessment

- Periodic reviews are performed to, among other things, anticipate and identify routine events or activities that may affect the entity's ability to achieve its objectives
  - Risks potentially affecting the achievement of financial reporting objectives are identified
  - Management identifies risks related to laws or regulations that may affect financial reporting
  - Risks related to the ability of an employee to initiate and process unauthorized transactions are appropriately identified
  - Management identifies all significant relationships including service providers
  - Periodic risk assessments are reviewed by management
  - Management develops plans to mitigate significant identified risks, including designing and implementing appropriate controls

Risk Assessment

- The entity considers the potential for fraud in assessing risks to the achievement of financial reporting objectives
- The entity's assessment of fraud risk considers incentives and pressures, attitudes, and rationalizations as well as the opportunity to commit fraud
- The entity's assessment of fraud risk considers risk factors relevant to its IT, including new applications and business processes
- The entity assesses the potential for fraud in high-risk areas, including revenue recognition, management override, accounting estimates, and nonstandard journal entries
- Those charged with governance (if separate from management) understand and exercise oversight of the entity's fraud risk assessment process

Risk Assessment

- The entity identifies and assesses changes that could significantly impact the system of internal control
- Management has established triggers for reassessment of risks as changes occur that may impact financial reporting objectives (e.g., new technologies, new accounting principles, nonroutine transactions, new products, etc.)

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question

Question 6: Multiple Choice

My clients:

A. **Perform technology risk assessments and diagnostics on a regular basis.**
B. **Do not believe it is necessary since they do not have sophisticated IT systems.**
C. **Understand that risk assessments and diagnostics are important but don't have the knowledge to do it or money to pay for it.**

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question

Question 6: Multiple Choice

My clients:

A. **Perform technology risk assessments and diagnostics on a regular basis.**
B. **Do not believe it is necessary since they do not have sophisticated IT systems.**
C. **Understand that risk assessments and diagnostics are important but don't have the knowledge to do it or money to pay for it.**

Answer: There is no correct answer to this question

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Auditor's Responsibility

- Auditors should inquire about management's risk assessment process including management's assessment of changes in its internal control and how they determined whether controls are in place to prevent, detect, and correct misstatement on a timely basis
- Auditors will need an understanding of changes to the processing environment as well as an understanding of the different technologies that a client may use in the financial reporting system

Auditor's Responsibility

- The auditor should consider:
  - New revenue streams;
  - Changes in the roles and responsibilities of entity personnel;
  - Automation of manual tasks;
  - Changes in staffing levels;
  - Changes in the way that the entity's systems are developed and maintained; and
  - How well the design and implementation of general computer controls addresses identified risks

Auditor's Responsibility

- The auditor will also want to talk with those charged with governance to see how the board, or audit committee, is overseeing the impact of emerging technologies on financial reporting
- If the entity has an internal audit department it is important to understand their role, if any, in IT auditing
- Auditors will want to understand:
  - Direct and indirect effects of the new technology and how it impacts audit risk;
  - How technologies impact the flow of transactions; and
  - The appropriateness of management's processes to select, develop, operate, and maintain controls related to the entity's IT

Auditor's Responsibility

- The auditor is less concerned with changes that are made to operational controls. Depending on the level of regulation in the entity's industry, the auditor may need to be concerned with changes made to internal controls over compliance since there could be an impact on compliance with laws and regulations

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 7: True or False

In order to assess risk, at a minimum, an auditor needs to obtain an understanding of changes to the processing environment and new technology that the entity is using in the financial reporting system. The auditor also needs to talk with those charged with governance and determine who is overseeing the impact of emerging technologies.

Discussion Question – True or False

Question 7: True or False

In order to assess risk, at a minimum, an auditor needs to obtain an understanding of changes to the processing environment and new technology that the entity is using in the financial reporting system. The auditor also needs to talk with those charged with governance and determine who is overseeing the impact of emerging technologies.

Answer: True

Information and Communication – *Application Controls*

- The COSO Framework includes three components related to IT controls:

1. **Application Controls**: Application controls are built into computer programs. They are designed to provide completeness and accuracy of information processing that is important to the integrity of the financial reporting process, authorization, and validity. They are specifically related to the classes of transactions and account balances
   - Application controls can be programmed
   - If the entity has an integrated ERP (enterprise resource planning) environment such as SAP, Oracle, or JD Edwards, many of the application controls will be programmed
   - Where the system is not quite so robust, the control objectives may be able to be satisfied by manual controls such as investigating exceptions or errors generated in processing

Information and Communication – *Application Controls* (Cont.)

- Overall control objectives of any IT application are to ensure:
  - Complete, accurate, valid data; and
  - Output that is distributed to authorized users
- Four broad types of application controls that are used to achieve the internal control objectives of the various cycles are:
  a. **Input controls** – Designed to ensure that the data entered into the system is complete and accurate
  b. **Processing controls** – Designed to ensure that data is processed completely and accurately, and data integrity is maintained while processing and in storage
  c. **Output controls** – Designed to ensure that reports produced by the system are distributed to only authorized personnel
  d. **Security controls** – Designed to ensure that data is stored and protected from unauthorized access, modification, or loss

Information and Communication – *General Computer Controls*

2. **General Computer Controls**: General computer controls are broad and include controls over:
   - Access;
   - Change and incident management;
   - Systems development;
   - Data backup and recovery; and
   - Physical security that is related to the integrity of financial reporting processes

- GCC contribute to the overall reliability of the information technology and are not related to a specific application

Information and Communication – *General Computer Controls* (Cont.)

- With many smaller entities, access control is often lacking
- Lack of access controls should be evaluated to determine how serious a deficiency it is
- Lack of access control may preclude reliance on both general and application IT controls and perhaps even manual controls
- At a minimum, the auditor should determine that:
  - Vendors can access the system only for a short period after installation;
  - Terminated employees no longer have access to the system; and
  - When job responsibilities are changed, access to data is also changed

Information and Communication – *End User Computing*

3. **End User Computing** includes the use of spreadsheets and other user-developed programs (such as databases) and involves:
   - Documentation of these programs;
   - Program security;
   - Back up; and
   - Regular review for processing integrity

Information and Communication – *End User Computing (Cont.)*

- Most midsize entities use packaged software products where the source code cannot be modified and where the software has limited connectivity to the Internet
- These entities will have less need for general and application computer controls such as delete, change, and incident management controls and systems development controls
- Auditor should determine that:
  - System updates were properly installed; and
  - New applications were tested and are running properly

Information and Communication – *End User Computing (Cont.)*

- Other entities use software programs that were developed in-house or by a local technology vendor where the entity has access to the source code
- This situation requires a larger array of general computer and application controls
- Auditors should be aware that if a company uses different software vendors for various applications, this will increase the risk of material misstatement

Technology Risks – Understanding Where Risk May Be Present

- Management and auditors should understand risks present due to specific programs or applications being introduced in the financial reporting system that are different than traditional systems
- Obtain sufficient knowledge of the information system including related business process relevant to financial reporting to understand:
  - Procedures used to initiate, authorize, record, process, and report information in the financial statements whether automated or manual
  - Related accounting records, whether electronic or manual, supporting information and specific accounts in the financial statements
  - How the information system captures events and conditions, other than classes of transactions that are routinely processed
  - Process used to prepare the entity's financial statements including significant accounting estimates and disclosures
  - Procedures and technology such as firewalls used to safeguard the entity's data
  - Extent of cybersecurity and access controls

Top Technology Risks

1. Reliance on systems that are inaccurately processing data or processing inaccurate data or both
2. Unauthorized access to data
3. A person may be given privileges that exceed their authority or are not compatible with their job function thereby diminishing the segregation of duties
4. Inappropriate changes could be made to systems of programs
5. IT personnel may make unauthorized or erroneous changes to data in master files

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Technology Risks

6. The entity may not make the necessary changes to systems or programs
7. Potential loss of data or inability to access data as necessary
8. Risks introduced when using third party service providers

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

1. Reliance on Systems That Are Inaccurately Processing Data or Processing Inaccurate Data or Both

- Management should select and develop control activities so that transaction processing is complete, accurate, and valid
- If the system has a feature where an alarm is triggered when there are issues, this will cause corrective action to be made
- But if not, then a manual review of system status and logs should be performed periodically. Timely corrective action is important
- Regular backups should be performed, and procedures developed to restore data if processing errors occur. The restoration process should be tested periodically

1. Reliance on Systems That Are Inaccurately Processing Data or Processing Inaccurate Data or Both

EXAMPLE

IT personnel in the data center at Holmes & Watson Financial Services monitor batch and real-time process of batch applications for errors using automated software. The scheduling software in the application checks for various problems including data errors and programs that do not complete properly or run out of order. An alarm feature alerts operators and business process owners to issues. Some of the company's applications are real time. Software is used to automatically monitor for error such as incomplete, inaccurate or invalid record transfers between systems. If the software detects a possible error, it attempts to resend the record. If the error persists, the system sends an email to an operator so they can correct the error. Financial management is notified of errors in a weekly report. This way adjustments can be made to the system if necessary. The controller reviews and approves changes to the systems.

2. Unauthorized Access to Data

- Risk of fraud or error
  - Destroy data
  - Make inappropriate changes to data
  - Record fictitious transactions
- If multiple users have access to a common database, it may be difficult to tell where the alteration originated

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

3. and 4. Incompatible Duties

3. A person may be given privileges that exceed their authority or are not compatible with their job function thereby diminishing the segregation of duties

4. Inappropriate changes could be made to systems or programs

- Networks, operating systems, databases, and applications supporting financially significant processes must support restricted access to financial applications and data in conformity with organizational policy
- This includes user authentication, access enforcement, and required parameters such as password format and a requirement to periodically change passwords

4. Inappropriate Changes Could Be Made to Systems or Programs

EXAMPLE

Accord Restaurant Supply (ARS), a distribution company, has several financially critical applications. Recently their external auditors reported a significant deficiency for poor infrastructure security controls. Password format requirements were not consistently applied, and some were below industry security standards. ARS designed a four-step remediation plan:

- Rate each application on its importance to financial reporting reliability;
- Specify security policies for each rating level;
- Assign each application a risk rating relating to its impact on financial reporting reliability; and
- Implement procedures to enforce policy compliance consistent with each application's ratings.

The external auditors also recommended that the entity perform an access audit every year to ensure that termination of access is made when a person leaves a position or the company. The access audit should also focus on whether the access given to personnel is appropriate and necessary for them to perform their duties.

Discussion Question

Question 8: Multiple Choice

Auditors are required to obtain an understanding of internal controls. The level of work depends on the significance and complexity of the system. Which is true about internal controls over technology?

A. Auditors need to address the general computer controls related to access and security regardless of the size and complexity of the client's information systems

B. An auditor does not need to worry about understanding internal controls over the client's information system if it is in the cloud

C. The auditor always needs to test internal controls over significant systems because of the level of risk in today's environment

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Discussion Question

Question 8: Multiple Choice

Auditors are required to obtain an understanding of internal controls. The level of work depends on the significance and complexity of the system. Which is true about internal controls over technology?

A. **Auditors need to address the general computer controls related to access and security regardless of the size and complexity of the client's information systems**

B. **An auditor does not need to worry about understanding internal controls over the client's information system if it is in the cloud**

C. **The auditor always needs to test internal controls over significant systems because of the level of risk in today's environment**

SURGENT ACCOUNTING & FINANCIAL EDUCATION

5. IT Personnel May Make Unauthorized or Erroneous Changes to Data in Master Files

EXAMPLE

A computer sales and service company believed that their internal controls over purchasing and payment were good, and that segregation of duties was adequate. However, since the entity was a midsize entity there were only 2 people handling information technology for the company. Jim reported to Bob and had the responsibility for assisting users and trouble shooting. Bob supervised Jim, made sure that updates to the system were installed, and authorized purchases. Bob was not required to have his work on the system reviewed since he was deemed a trusted employee and very skilled. While preparing for the financial statement audit the CFO noticed an unusual fluctuation in an expense account. Upon investigation it appeared that a vendor was established in the master vendor file outside the normal approval process. Bob had inappropriate access and had inserted a fictitious vendor. He had been embezzling from the company for several years.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

6. The Entity May Not Make the Necessary Changes and Updates to Systems or Programs

EXAMPLE

A healthcare provider's charges were determined by a charge master. They accepted various forms of insurance as well as Medicare and Medicaid. The revenue that the entity could expect to collect was dependent on a fee schedule that changed periodically. The provider accessed the electronic fee schedule when the changes were scheduled to take effect. The employee responsible for monitoring software updates was in an accident and was not able to work for 2 months. The updates were not made during that time. The employee responsible for the updates was also not there to install the regular systems software updates that contained patches and other improvements. Fortunately, the situation only resulted in errors in revenue that were detected during the monthly review.

7. Potential Loss of Data or Inability to Access Data as Necessary

- Data availability means that data/information is accessible to authorized users whenever it is needed
- For many companies this is a significant concern. The loss of the ability to process diminishes the productivity and effectiveness of the entity
- For some companies, for example in the healthcare space, the inability to access information when needed can be life threatening
- A good source to look regarding internal controls is in the AICPA Trust Principles, which are used in establishing criteria for service organizations

7. Potential Loss of Data or Inability to Access Data as Necessary

- There are three principles related to data availability:
  - A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives
  - A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives
  - A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives

7. Potential Loss of Data or Inability to Access Data as Necessary

- Following are example controls that could be implemented that would be responsible to the principles identified above:
  - **Current Usage** – Measurement of use of system components is performed to establish a baseline for capacity management and to refer to when evaluating the risk of lack of availability due to capacity constraints
  - **Forecasts Capacity** – A forecast and comparison of expected average and high use of system components to system capacity and tolerances is performed. Considerations include capacity in the event there is a system failure
  - **Identifies Environmental Threats** – Management identifies environmental threats as part of the risk assessment that could impair the availability of the system. These could include threats resulting from weather, failure of environmental control systems, electrical discharge, fire, and flood/water

→

7. Potential Loss of Data or Inability to Access Data as Necessary

- Following are example controls that could be implemented that would be responsible to the principles identified above (cont.):
  - **Designs Detection Measures** – Measures are implemented for detecting anomalies that could result from environmental threat events
  - **Implements and Maintains Environmental Protection Mechanisms** – Environment protection mechanisms are implemented by Management to prevent and mitigate against environmental events
  - **Responds to Environmental Threat Events** – Procedures have been developed and put in place for responding to environmental threats and for evaluating the effectiveness of those policies and procedures on an ongoing or periodic basis. This includes, but is not limited to, automatic mitigation systems (i.e., UPS and generator back-up subsystem)

→

7. Potential Loss of Data or Inability to Access Data as Necessary

- Following are example controls that could be implemented that would be responsible to the principles identified above (cont.):
  - **Implements Business Continuity Plan Testing** – Business continuity plan testing is performed on at least an annual basis. The testing includes: (1) developing testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from the entire entity that can impact availability; (3) scenarios that consider the potential for lack of availability of key personnel; and (4) updating continuity plans and systems based on test results
  - **Tests Integrity and Completeness of Back-Up Data** – The integrity and completeness of back-up information is tested on at least an annual basis

8. Risks Introduced When Using Third-Party Service Providers

- Various risks can be introduced when the company uses an outsourced service provider
- Management should obtain a SOC 1 report from the service provider and read it to determine whether there are any significant issues with the service provider's system of internal control that would impact the company's financial reporting
- A SOC 1 type 2 report is preferable to a type 1 report because in a type 2 report, the auditor reports on a period of time and addresses the fairness of the presentation of management's description of the system, the suitability of the design, and the operating effectiveness of the controls
- Management should evaluate the suggested complementary user controls and ensure that the controls that the company has in place are adequate
- Management should also consider cybersecurity, data access, and vendor risk considerations associated with the service provider

8. Risks Introduced When Using Third-Party Service Providers

EXAMPLE

Puppy Playscapes is a franchisor of pet day care centers across the country. It outsourced its ERP application to a cloud-based service provider. Before doing so management requested a SOC 1 report from the service provider. The controller reviewed the report and noted that this was a type 2 report so the controls at the service provider were evaluated for design as well as operating effectiveness. The controller assessed the risks associated with the outsourced arrangement and believed that the service organization's quality was good.

8. Risks Introduced When Using Third-Party Service Providers

Puppy Playscapes Example (cont.)

Each year the system of internal controls required that management obtain a current SOC report. In 20X1, the controller obtained the current report and identified several issues that needed to be addressed. The report did not include certain controls that were customized especially for the business practices of Puppy Playscapes. To address this concern management decided to develop controls at their company to address the related financial reporting risks. The report did not cover all 12 months of the company's year-end. There was a 2-month gap. The controller evaluated the risk and decided that he would have company personnel perform corroborative inquiry with the service provider to see if there were any changes between the last date covered by the report and the company's year-end.

There were two exceptions noted in the report. According to the service auditor, those issues were retested, and the controls found to be effective. One of the exceptions was not significant. The other was but the controller determined that the existence of a complimentary user control at the company was sufficient to mitigate the problem.

Third-Party Service Providers

Even when no SOC 1 report is available management should still address the control activities at the service organization.

EXAMPLE

Higher Life Foundation (HLF) has a significant endowment. It outsources the investment management activity to Canton Financial Management Company (CFMS). There is no service organization control report available. However, HLF has heard favorable reports of CFMS.

The management of HLF evaluates the nature of the control activities of CFMS and also evaluates its own control activities. Management determines that the risk of material omission or misstatement is high so additional procedures will be necessary on the part of management at the beginning of the relationship as well as on an ongoing basis. HLF arranges for its internal audit group to conduct certain tests of controls at CFMS. In addition, management evaluates its own user control activities to ensure that they are sufficient. Management added monitoring controls to the ones currently in place.

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Cybersecurity Risks

- "There are only two types of companies: those that have been hacked and those that will be hacked"
  - – The late Robert S. Mueller, III, former Director of the FBI
- The average cost of a data breach was $4.88 million in 2024, the highest average on record (IBM)
- In 2023, security breaches saw a 72 percent increase from 2021, which held the previous all-time record (Forbes)
- In 2022, the Federal Trade Commission received more than 1.1 million reports of identity theft (US News)
- 64 percent of Americans have never checked to see if they were affected by a data breach (Varonis)

Evolving Cyber Fraud Threats

- Threat actors are leveraging AI to create fake invoices, impersonate executives, and exploit processes
- Procurement fraud is now among the top three most disruptive economic crimes across industries[1]
- Many companies still underutilize data analytics in fraud detection
- Criminals rapidly adapt to new controls with more sophisticated attacks
- Response strategies:
  - Strengthen internal controls and vendor due diligence
  - Increase employee fraud awareness
  - Use real-time monitoring and AI-based detection
  - Invest in cyber fraud insurance

1. PwC's 2024 Global Economic Crime Survey

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

- Authorized Push Payments (APPs)
  - Victims are manipulated into making real-time payments to fraudsters
  - Occur due to social engineering attacks involving impersonation
  - Convince business or person to send money to them for what appears to be a legitimate purpose
  - Victim authorizes bank to make payment to fraudster's bank account
  - Push payments are used to cut time off transactions
  - Common in real estate transactions
  - Prevalent scheme in the UK now being seen in US
- SMS Spoofing is a technique to commit APP fraud using technology to impersonate a trusted party

Authorized Push Payment – Example

EXAMPLE

A threat actor is aware that a customer is about to purchase a home. Through phishing or social engineering, they cause the customer to create an authorized push payment but instead of the money ending up in an escrow account or the seller's account it goes to a fraudulent account. Because it was authorized the bank has no responsibility. By the time it is evident that this has occurred the money has long been forwarded to a place where it generally cannot be reclaimed. Payment service providers (PSP) have created software to detect unusual behavior and have even helped to try to reclaim money for victims

Top Cyber Fraud Schemes

- Deep fakes and biometrics
  - Facial recognition used to unlock cell phones
  - Voice biometrics to command smart home devices
  - Criminals use artificial intelligence to create fake images or audio manipulations

EXAMPLE

"A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police" – CNN (February 2024)

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

- Breaching MFA
  - Multi-factor authentication
  - Use of SIM swapping to circumvent the control

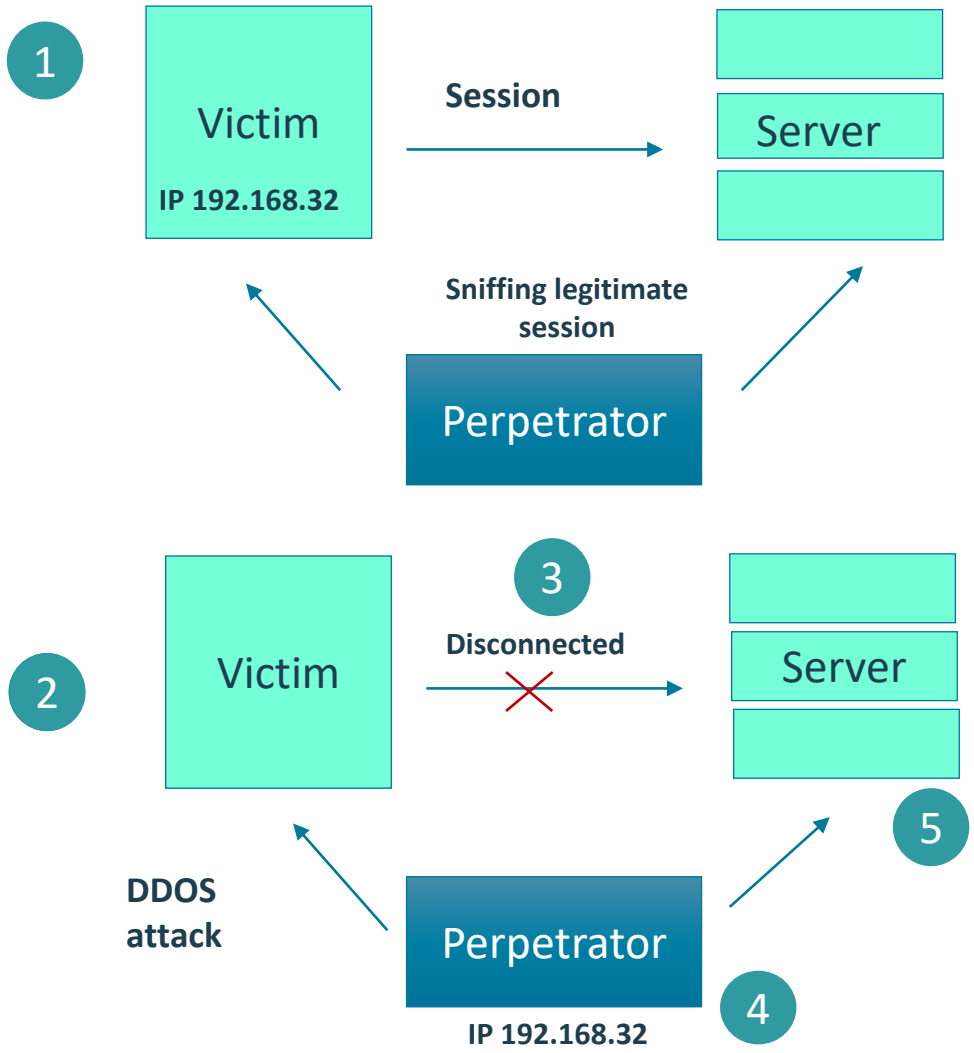
EXAMPLE

A threat actor visited a retail store of a mobile service provider. The fraudster reported a device (not hers) as lost. She asked the provider to activate a new SIM card with a phone number that was not hers. She had convincing identification and the store clerk activated on the criminal's device which she said was a spare phone. This enabled the fraudster to circumvent MFA since she would get the call instead of the real mobile customer.

Top Cyber Fraud Schemes

- Denial-of-service and distributed denial-of-service
  - Attacks overwhelm a company's information system's resources so that it is not able to respond to service requests
  - DDoS attack is launched from a large number of other host machines that are infected by malicious software controlled by the attacker
  - Threat actor doesn't gain access to a system
  - Goal is simply to take a system offline
  - Used against competitor or to disrupt a system so that the threat actor can launch another type of attack

TCP SYN Flood Attack



1. A client connects to a server
2. The attacker's computer gains control of the client
3. The attacker's computer disconnects the client from the server
4. The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers
5. The attacker's computer continues dialog with the server, and the server believes it is still communicating with the client

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Denial of Service and Distributed Denial of Service

1. TCP SYN flood attack solutions:
   - Place servers behind a firewall configured to stop inbound SYN packets; or
   - Increase the size of the connection queue and decrease the timeout on open connections
2. Teardrop attack
   - Causes the length and fragmentation offset fields in sequential Internet Protocol (IP) packets to overlap one another on the attacked host
   - When the attacked system attempts to reconstruct packets during the process it fails, becomes confused and crashes

Denial of Service and Distributed Denial of Service

3. Smurf attack
   - Uses Internet Protocol (IP) spoofing and the ICMP (internet control message protocol) to saturate a target network with traffic
   - Threat actors use IP spoofing to convince a system that it is communicating with a known, trusted entity
   - Threat actor sends a packet with the IP source address of a known, trusted host instead of its own IP, providing the attacker with access to the system

- There are patches available for this type of attack. Alternatively, the entity could disable SMBv2 and block ports 139 and 445

EXAMPLE

The victim address is 10.0.0.10. The threat actor spoofs an ICMP echo request from 10.0.0.10 to the broadcast address 10.255.255.255. The request goes to the IPs in the range. The responses go back to 10.0.0.10 and overwhelms the network.

Denial of Service and Distributed Denial of Service

4. Ping of Death
   - The threat actor uses IP packets that are over the maximum size to “ping” a target system
   - IP packets of this size are not allowed so the attack will fragment the IP packet
   - Once the target system reassembles the packet, it can experience buffer overflows and other crashes

- Ping of death attacks can be blocked by using a firewall that will check fragmented IP packets for maximum size

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Denial of Service and Distributed Denial of Service

5. Botnet
   - Group of computers that have been infected by malware and are under the control of a fraudster
   - Term bot refers to the infected device
   - Can be designed for illegal or malicious tasks such as sending spam, stealing data, ransomware, or DDoS attacks
   - When used in a DDoS attack the bots carry out attacks against the target systems, overwhelming the target system's bandwidth and processing capabilities

- Bots can be mitigated by RFC3704 and black hole filtering

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Denial of Service and Distributed Denial of Service

6. Ransomware and Ransom Attacks
   - Ransomware is malware that infects IT systems, halting user activity until a ransom is paid
   - Ransomware is not new. At one time, threat actors required payment through the U.S. mail
   - As technology has progressed, payment is generally demanded by bitcoin or credit card. Law enforcement officials recommend that a victim refuse to pay the ransom
   - The malware often enters the system through phishing email
   - Largely would not exist without cryptocurrencies (e.g., digital currency) that allow anonymous payments and receipts

Top Cyber Fraud Schemes

6. Ransomware and Ransom Attacks (cont.)
   - DDoS and ransom attacks are often linked. Ransom attacks take two forms
   - In some instances, the threat actors threaten to launch a DDoS attack on an organization's site unless the organization pays a ransom fee in bitcoin
   - In other instances, threat actors infect machines in a network with crypto-ransomware that encrypts all files, then demand a ransom fee to unlock the files
   - One solution to deal with ransomware is to back up the system hourly on an unrelated server

Top Cyber Fraud Schemes

- Phishing and Spear Phishing attacks

  Phishing – Threat actor sends emails that appear to be from trusted sources with the goal of gaining personal information or convincing users to do something

  - Combines social engineering and technical trickery
  - Could involve an attachment to an email that loads malware onto a computer
  - Could appear to be a link to a website that tricks the victim into downloading malware or providing the threat actor with personal information

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

- Spear phishing is a specific type of phishing activity
  - Threat actors research the habits and language of the victim and craft emails that are personal and relevant
  - Threat actors may use email spoofing
  - Information in the “From” section appears to come from someone known to the victim, generally someone with the authority to issue instructions
  - Another technique that threat actors use is website cloning. The threat actor copies a legitimate website, and the victim enters personally identifiable information (PII) or login credentials
  - Phishing attacks increasingly use generative AI to create more convincing messages and may be associated with business email compromise (BEC) schemes or QR-code phishing (“quishing”)

→

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

Solution

- **Stop and think** – Analyze email and don't just accept that it is from the person who is purported to have sent it. People tend to react to email without thinking
- **Hover over the email headers or links in the message** – Move the mouse over the link without clicking on it. It is possible that the email address or links are spoofed
- **Analyzing email headers** – Email headers define how an email got to your address. The "Reply-to" and "Return-Path" parameters should lead to the same domain as is stated in the email
- Use extra caution with QR codes, especially when they appear in emails, invoices, or unexpected messages

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

Drive-by download attacks

- Common method of spreading malware
- Threat actor looks for an insecure website and places a malicious script into the code on one of the pages
- Script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the threat actors
- Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

Drive-by download attacks

- Drive-by doesn't rely on a user to do anything to actively enable the attack making it harder to prevent
- Can take advantage of an app, operating system, or web browser that contains security flaws due to unsuccessful updates or lack of updates

- Browsers and operating systems should be kept up to date and insecure websites should be avoided. The more apps or plug-ins someone has on their device, the more vulnerable they are

Top Cyber Fraud Schemes

- **Password Attacks**
  - Threat actors will sometimes look around a person's desk if they are in the same location
  - Alternatively, they may "sniff" the connection to the network to acquire unencrypted passwords, use social engineering, gain access to a password database, or simply guess
  - **Brute-force** or targeted password guessing – Automated attempts to try many possible passwords or personalized guesses based on information known about the user
  - **Dictionary attack** – The threat actor copies an encrypted file that contains the passwords, applies the same encryption to a dictionary of commonly used passwords, and compares the results

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

- **Cross-site Scripting Attacks (XSS)**
  - Use an entity's website to run scripts in the victim's web browser or scriptable application
  - Threat actor exploits a vulnerability in a website that is otherwise benign
  - Victim visits the website and clicks on a page causing a malicious JavaScript which was originally inserted in the target website to execute a malicious script
  - At best the threat actor can then hijack the session
  - At the worst, a threat actor can steal cookies, log keystrokes, capture screen shots, collect network information, and remotely access and control the victim's machine

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

- **Cross Scripting Attacks (XSS) – Solutions**
  - Web developers can sanitize data input by users in an HTTP request before reflecting it back
  - Make sure all data is validated, filtered or escaped before echoing anything back to the user, such as the values of query parameters during searches
  - Give users the option to disable client-side scripts

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

- **Eavesdropping**
  - Intercept network traffic
  - The threat actor's goal is to obtain passwords, credit card numbers and other confidential information that a user might be sending over the network
  - When eavesdropping is passive, the threat actor finds information by listening to the message transmission in the network
  - Threat actors can also actively eavesdrop by camouflaging themselves as a friendly unit sending queries to transmitters. In order to launch an active attack, the threat actor must first gain knowledge of friendly units
  - **Solution:** Data encryption is the best way to counteract eavesdropping

Top Cyber Fraud Schemes

- **Malware**
  - **Macro viruses** infiltrate programs most people use every day such as Microsoft Word or Excel
    - Viruses attach themselves to an application's initialization sequence. When a person opens the application, the virus gives the malicious instructions before transferring control to the application. This way it can replicate itself and attach to other code in the victim's system
  - **File infectors** attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded

Top Cyber Fraud Schemes

- **Malware**
  - **System or boot-record infectors** attach to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can spread to other disks and computers
  - **Stealth viruses** compromise malware detection software so that the software will report an infected area as being uninfected
  - **Trojan horses** hide in a useful program. They have a malicious function but do not self-replicate. They are used by threat actors to infiltrate a system but also have another feature whereby they can establish a back door that can be exploited by the threat actor

Top Cyber Fraud Schemes

- **Malware**
  - **Worms** do not attach to a host file
    - They are self-contained programs that spread across networks and computers, usually through email attachments
    - Victim opens an attachment and activates the worm program
    - Worm then sends a copy of itself to every contact in the victim's email program. This enables it to spread itself across the internet, conduct malicious activity and overload email servers which can result in DOS attacks
  - **Ransomware** is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid

Top Cyber Fraud Schemes

- **Internet of Things (IoT)**
  - **Extends connectivity beyond normal devices to household devices and other objects**

Group	Application
Consumer	**Smart security, smart speakers, smart air conditioning, pace makers, smart watches that collect health data, garage door openers, smart TVs, toys**
Enterprise	**Commercial security systems, traffic monitors, smart lighting, smart air conditioning, conference room locaters set up for temperature that adjusts based on occupancy, lights that dim as presentation is loaded on a screen**
Industrial	**Assembly line machine provides data to the plant operator on anomalies predicting when parts need to be replaced. Drones and other devices used by the military.**

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Top Cyber Fraud Schemes

- **It's Also a People Problem**
  - Social engineering is responsible for 93 percent of data breaches
  - Threat actors generally use social engineering to gain access to passwords, bank information or a computer so they can install malware to give them access to a lot more
  - When the threat actor manages to obtain access to one person's password, they have access to that person's contact list. They can then use the email account of the first victim to send emails to the person's contacts
  - Links can be embedded in the emails, and if it appears that the email is a trusted source, then clicks on the link give the threat actor a second victim
  - The email could also have a download of music, movies, or documents with embedded malware

Top Cyber Fraud Schemes

- Hovering over the email address to see if it is legitimate may not be completely effective since threat actors can also camouflage their true email addresses with overlays
- Threat actors frequently impersonate companies, and the emails look legitimate right down to the logos and key words that the bank might use
- According to Webroot data, financial institutions are the most often impersonated
- Threat actors will ask for donations, present an issue and ask the victim to validate information by providing information in a form or clicking on a link, offer something free, respond to a question the victim never asked, claim that the victim is winner of some prize or pose as a co-worker, boss, company executive, etc.

→

Top Cyber Fraud Schemes

Solutions

- Slow down. Nothing is that urgent that it should not be carefully reviewed
- Ask for oral verification even if it slows down the process. Call the sender and ask
- Go straight to the website of the financial institution purporting to be the sender in a fresh browser and see if there are any messages waiting there
- Delete any requests for financial information or passwords
- Scams come in the form of offers to help, e.g., to restore credit scores, refinance a home, etc. Delete them

Top Cyber Fraud Schemes

Solutions

- Secure computing devices with anti-virus software, firewalls, email filters, and update them regularly
- Companies should train employees and penalize them for disregarding policies and procedures on information security

EXAMPLE

The controller of a company was aware that she would be asked to make a wire transfer in connection with a transaction in the next few days. This transaction had been the subject of discussion between her and the CFO. She was not surprised when she got an email, purportedly from the CFO with wiring instructions. She made the transfer as requested. Unfortunately, she learned that she had made a mistake when the CFO called her on the phone several hours later to let her know he was sending instructions. The threat actor had been eavesdropping in the system learning the language that the CFO would use communicating with the controller and waiting for the appropriate time to make a move.

Top Cyber Fraud Schemes

EXAMPLE

An employee working in accounts payable received a message from a “vendor” providing new routing information for payments. The email message had the logo, color palette and wording of the legitimate vendor company. In addition, it was from someone that the employee “knew.” The attachment with the new information appeared legitimate as well. The employee made the change not realizing that the request was coming from an attacker that was using social engineering techniques. Unfortunately, they were effective, and the company sent payments for several months to this fictitious account before they were contacted by the real vendor asking why payments had not been made.

Top Cyber Fraud Schemes

- Employees may inadvertently play a role in cybercrime
  - 91 percent of malware was delivered by email (Deloitte)
  - 19 percent of 2022 data breaches caused by stolen/compromised credentials (IBM 2022)
  - Phishing levels declined to only 16 percent of breaches in 2022 (IBM 2022)
    - However, they were the costliest, averaging almost $5 million per breach
    - Second costliest was business email malware attacks at $4.89 million
  - 45 percent of data breaches occurred in the cloud (IBM 2022)
  - 83 percent of organizations had more than one data breach (IBM 2022)
    - Average total cost was $4.35 million per breach in 2022

Internal Control Imperative

Key Lessons from SEC Cyber Fraud Cases

- The SEC has investigated multiple cyber-enabled cases involving nearly $100 million in losses across nine companies[1]
- The techniques used by the fraudsters are common
  - Company personnel received spoofed or compromised electronic communications from external sources, leading them to transfer funds to the fraudsters' bank accounts
- One company made 14 electronic transfers based on fictitious emails received from fraudsters masquerading as company executives
- Another company paid 8 invoices over several months to what they believed were legitimate vendors. However, the routing instructions had been changed to a fraudster's bank account

1. "SEC Investigates Cyber-Related Frauds Perpetrated Against Public Companies," Press Release No. 2018-236

Internal Control Imperative

- The SEC did not institute enforcement actions against the companies but made it clear in the report that public companies will be required to assess and adjust their internal controls for the risk of cyber fraud
- The SEC requires companies to disclose material cybersecurity incidents as of December 15, 2023
- Section 13(b)(2)(B) of the Securities Exchange Act is invoked when a public company has:
  - Materially misstated its financial statements;
  - Paid bribes to foreign government officials;
  - Paid commercial bribes; or
  - Reimbursed employees for unauthorized expenses

Discussion Question – True or False

Question 9: True or False

Social engineering is still a problem that companies face even when personnel have been trained. One reason for this is that people may be moving too fast and not carefully reviewing an email before clicking on it.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 9: True or False

Social engineering is still a problem that companies face even when personnel have been trained. One reason for this is that people may be moving too fast and not carefully reviewing an email before clicking on it.

Answer: True

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 10: True or False

Ransomware is malware that is typically installed by a program when an employee enters a fictitious website.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 10: True or False

Ransomware is malware that is typically installed by a program when an employee enters a fictitious website.

Answer: False, ransomware generally enters the system through phishing email.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

SEC Cyber Fraud Report

- Most prosecutions have involved public companies engaged in accounting fraud
- Internal control charges were levied as lesser included offenses
- The SEC's report has now opened the possibility for charges to be made when a public company is victimized by a cyber incident and unknowingly disburses funds to cyber threat actors
- Sections cited would be Section 13(b)(2)(B)(i) and (iii)
  - These are the sections that require the execution of transactions and access to company assets to be permitted with management's general or specific authorization
  - Used by the SEC in connection with bribery and expense reimbursement prosecutions where the financial ramifications are generally not material for financial statement purposes

Internal Control Imperative

- Cases discussed in the report did not involve sophisticated schemes
- Human weakness made them effective
- COSO framework is specific in saying that controls only provide reasonable, not absolute assurance
- SEC report is sobering to read and although ultimately prosecution may only occur when it is evident that internal controls were blatantly ignored, companies should take proactive steps to identify the risk of cyber fraud
- Includes nonpublic entities as well, even only if it is because cyber fraud is costly to an entity's financial position and reputation

Internal Control To Help Prevent Cyber Fraud

- Entities should consider:
  - A robust cyber fraud risk assessment process
  - Establishing more stringent cybersecurity policies and procedures
  - Performing scenario analysis including how management could override controls
  - Identifying key controls to prevent improper disbursements or accounting errors from cyber fraud focusing on payment requests, authorizations and disbursement approvals especially for large, nonsystematic, time sensitive or foreign transactions

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Internal Control To Help Prevent Cyber Fraud

- Entities should consider:
  - Identifying key controls over changes to vendor disbursement processes
  - Evaluating the design and periodically testing controls
  - Obtaining a cyber fraud diagnostic from a qualified third-party provider
  - Training personnel and penalizing those who violate the controls even through carelessness
  - Monitoring activities with data analytic tools for potential improper disbursements
  - Requiring independent verification for vendor banking changes, urgent payment requests, and other high-risk disbursements

Internal Control To Help Prevent Cyber Fraud

Type	Purpose	How It Works
Multifactor authentication (MFA)	Used to validate that authorized users are authenticated before gaining access to the system	Implementation of application-based MFA for hosted email solutions. MFA can help prevent a threat actor from accessing a hosted email solution that would then be used by the threat actor to send emails from a compromised company email address
Virtual private network	Controls are implemented to restrict VPN access to authorized and appropriate users	Many organizations already use VPN to authenticate users who attempt to gain access to an organization's internal network from a mobile location. Applications and infrastructure are placed behind the organization's firewall and are therefore unable to be accessed until the users connect to the VPN
Secure email gateways	Controls are implemented to encrypt and decrypt email to prevent unauthorized disclosure of information	Strong security controls associated with inbound and outbound email traffic are necessary to help prevent unauthorized disclosure of information
URL filtering	Controls are implemented to restrict malicious material from being delivered over a web browser or email	Preventing users from accessing malicious web addresses helps avoid unauthorized disclosure of sensitive information, such as the username and password of an employee used for authentication. Preventative controls in the email gateway further reduce the likelihood
Endpoint security	Endpoint protection (antivirus, anti-malware) is implemented to prevent malicious software from running	If enterprise-wide preventative controls fail to detect and mitigate the threat before a user sees it, endpoint protection may add an additional manipulation step to prevent unauthorized use of computer resources

Discussion Question – True or False

Question 11: True or False

According to the October 2018 SEC report, the SEC will now be penalizing companies with large fines whenever they experience material cyberfraud and it could have been prevented by more robust internal controls.

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Discussion Question – True or False

Question 11: True or False

According to the October 2018 SEC report, the SEC will now be penalizing companies with large fines whenever they experience material cyberfraud and it could have been prevented by more robust internal controls.

Answer: False. The SEC report opened the possibility of charges to be made against a public company that is victimized by cyber fraud but according to the report ultimately prosecution would only occur when controls are blatantly ignored.

Internal Control Imperative

- Specific Industry Statistics:
  - 43 percent of cyber attacks target smaller businesses (UNG)
  - 95 percent of breached records came from 3 industries: government, retail, and technology (UNG)
  - Manufacturing saw the highest share of cyber attacks in 2022, representing 24.8 percent of attacks; next was finance/insurance at 18.9 percent of attacks (Statista)
  - 75 percent of healthcare industry had a malware infection (UNG)
  - Industrial organizations saw an 87 percent increase in ransomware attacks in 2022 (Bloomberg)

Internal Control Imperative

Discussion questions:

1. Which of the fraud types have you seen occur in your company (your clients)?
2. How prepared do you believe your company (your clients) is/are for these possible attacks?

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

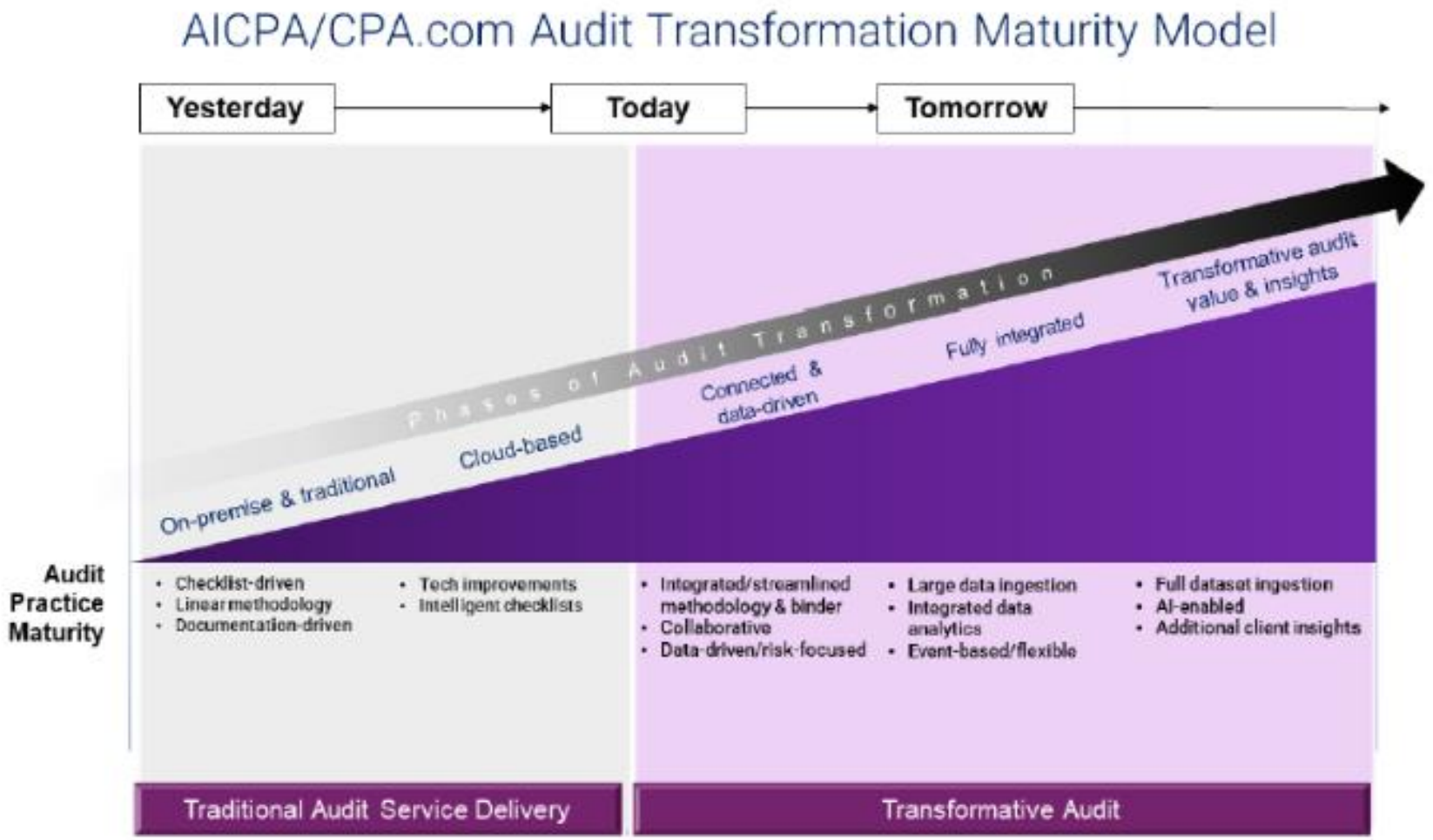
Audit Transformation

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Audit Transformation

- Traditionally, audits relied on document-checklist methods
- The adoption of cloud computing, AI, and data analytics has transformed these traditional methods, enhancing audit efficiency and effectiveness
- Auditors are moving into the next phase of audit transformation, as illustrated by the “AICPA/CPA.com Audit Transformation Maturity Model”
- The field is expected to progress with further enhancements and deeper insights into audit engagements
- Future developments will be driven by auditors adopting fully integrated, knowledge-driven methodologies that utilize AI and other advanced technologies

Audit Transformation



SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Audit Transformation

- The AICPA has long advocated for integrating technology to revolutionize the audit process
- As part of this initiative, the AICPA has collaborated with CPA.com, leading accounting firms, and Caseware International to develop the Dynamic Audit Solution (DAS)
- DAS integrates a data-driven methodology, guided workflow tools, and data analytics into a single cloud-based platform
- The initiative helped accelerate broader adoption of data-driven audit methodologies, cloud-based audit platforms, and integrated analytics tools across the profession

Audit Transformation

- A recent practice aid from the ASB's Technology Task Force, "Use of Technology in an Audit of Financial Statements," helps auditors refine their risk assessments. The document uses examples to show how technology can improve audit effectiveness and efficiency, focusing initially on risk identification and assessment per Statement on Auditing Standards (SAS) No. 145
- Auditors remain responsible for exercising professional skepticism and evaluating whether AI-assisted or technology-generated outputs provide sufficient appropriate audit evidence

Audit Documentation

- Audit documentation is very important in all audits but particularly where new audit techniques are used
- It is highlighted by the AICPA as an important component of SAS 142. However, AU-C 230 was not amended as a result of the standard
- As in all audits, the auditor should prepare audit documentation that is sufficient to enable an experienced auditor, having no previous connection with the audit, to:
  - Understand the nature, timing, and extent of the audit procedures performed;
  - Comply with professional and legal requirements; and
  - Provide a record of the results of the audit procedures performed and the audit evidence obtained

Documentation

- Documentation should include discussion of instances where significant findings or issues arose during the audit, the conclusions reached about those issues, and significant professional judgments made in reaching those conclusions
- The auditor should document:
  - The identifying characteristics of the specific items or matters tested;
  - Who performed the audit work and the date such work was completed; and
  - Who reviewed the audit work performed and the date and extent of such review
- Abstracts or copies of significant contracts or agreements should be included in the workpapers

Documentation

- The auditor should document discussions of significant findings or issues with management, those charged with governance, and others, including the nature of the significant findings or issues discussed, and when and with whom the discussions took place
- Since audit data analytics can yield results that are different from recorded balances, SAS 142 specifically highlights the need to document areas where these discrepancies occur, the auditor's investigation of those instances, and how the auditor addressed the inconsistency
- When auditors use AI-assisted tools, automated analytics, or other emerging technologies, audit documentation may need to address the procedures performed, the source of the information used, significant judgments made in evaluating the results, and any validation or corroborative procedures performed to support the reliability and appropriateness of the resulting audit evidence

Thank you!

SURGENT
ACCOUNTING & FINANCIAL EDUCATION