Technology Trends and Hot Topics Impacting the Accounting Profession

THT4/26/V1

201 N. King of Prussia Road
Suite 370
Radnor, PA 19087
P : (610) 688 4477
F : (610) 688 3977
info@surgent.com
surgentcpe.com

SURGENT
ContinuingEducation

Calling All **Exceptional**
INSTRUCTORS

Surgent is currently accepting nominations

for prospective new Discussion Leaders in the following areas:

Tax

Accounting & Audit

Gov't and Not-for-Profit A&A

Business and Industry
(all topics)

If you are an experienced CPA, have strong public speaking and teaching skills, and an interest in sharing your knowledge with your peers by teaching live seminars, we would love to hear from you!

Interested in becoming a Surgent discussion leader?

Reach out to us at
recruitment@surgent.com

SURGENT
ContinuingEducation

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

SURGENT FOR ENTERPRISE

Educational Solutions that Advance the Strategic Value of Everyone in Your Firm

At Surgent, we tailor our offerings—**exam review**, **continuing education**, and **staff training programs**—to meet your organization's specific needs in the most convenient and effective ways possible.

Personalized Exam Review

Help associates pass faster with the industry's most advanced exam review courses

- Adaptive study model offered for CPA, CMA, EA, CISA, CIA, and SIE exams
- Monitor employees' exam review progress with Firm360

Continuing Professional Education (CPE)

Make CPE easy for you and your staff with several ways to buy, earn and track CPE

- Flex Access Program – Secure a pool of CPE hours your staff can pull from in live webinar and/or self-study format
- Onsite Training – Reserve an in-firm training with a Surgent instructor
- Course licensing – License content from Surgent to lead your own CPE training

Staff Level Training

Leverage highly practical sessions, organized into suggested curricula according to staff experience levels

- Audit Skills Training Program
- Internal Audit Training Program
- Taxation Training Program

FIRM CPE PORTAL

Track and manage CPE for all users in your organization quickly and easily with Surgent's Firm CPE Portal.

Request a demo today!

Every firm is unique—and that is why we built our customizable, innovative Surgent for Enterprise program.

Contact our Firm Solutions team today to learn how Surgent can partner with you to create a solution to support staff development for your organization.

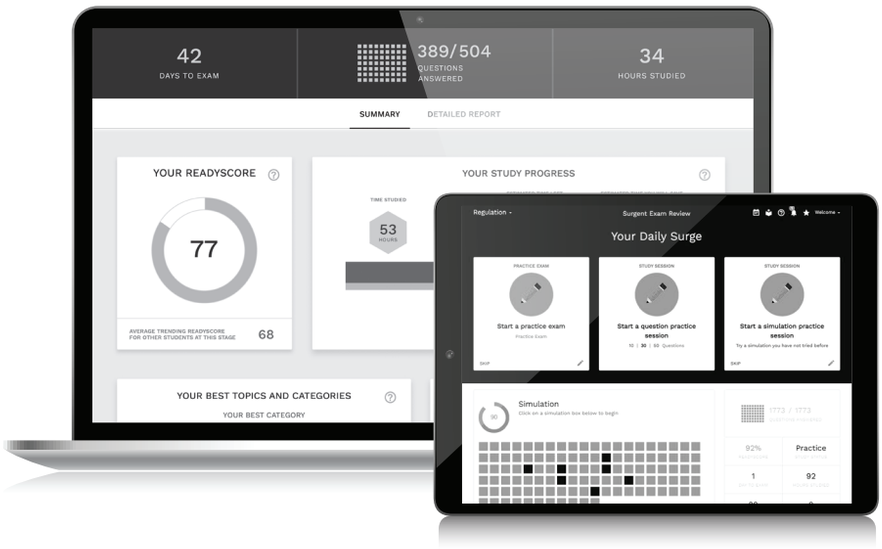
(484) 588.4197
salesinfo@surgent.com

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

STUDY LESS AND PASS FASTER

with the industry's most advanced exam prep courses

Surgent's AI-powered software personalizes study plans for each student, targeting knowledge gaps and optimizing those plans in real-time. This award-winning approach has been shown to save candidates hundreds of hours in study time.



KEY FEATURES

READYSCORE

Know what you're going to score before taking the exam.

PERFORMANCE REPORTS

Leverage your dashboard to know how you're doing every step of the way.

PASS GUARANTEE

If you fail your exam after using our course, we'll refund your money.

A.S.A.P Technology

helps you pass the

- **CPA** Exam
- **CMA** Exam
- **EA** Exam
- **CIA** Exam
- **CISA** Exam
- **SIE** Exam

Leading education for your firm? Surgent offers preferred partner pricing, coaching and more support methods to our firm clients and their staff. **Contact our Firms Solutions team today at salesinfo@surgent.com.**

Ready to explore exam prep course packages from Surgent? **Visit surgent.com to learn more!**

Table of Contents

Data-Driven Decision-Making 1

Technology Trends and Risks.....2

Revised June 2026

NOTES

Data-Driven Decision-Making

Learning objectives 1
I. Introduction 1
A. Disruptive technologies 2
B. Drivers of change in a digital world 2
II. Becoming a data-driven organization 3
A. Key to digital transformation 4
B. Why this is important to finance and accounting 4
C. Data-driven decision-making 4
1. Benefits of data-driven decision-making 4
2. Challenges and barriers with data-driven decision-making 5
D. Steps to become a more data-driven decision entity 6
1. Decide what to measure 7
2. Choose the correct BI Tools 7
3. Identify the correct personnel to analyze data 8
4. Address the issue of decentralized data 8
5. Data security and data integrity 8
6. Culture shift 9

Data-Driven Decision-Making

Learning objectives

Upon completing this chapter, the reader will 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.

I. Introduction

Companies are under an immense amount of pressure today. The business environment continues to be increasingly complex, and the changes are magnified by global, demographic, and regulatory factors, not to mention the rapid advancement in technology. Companies are witnessing increased competition coming from not only the competitors they were aware of but also from competitors they never expected. Industry research[1] reveals significant developments shaping the accounting profession, focusing on challenges posed by new technologies and the increasing significance of advisory services. The report identifies that 67 percent of accounting firms now classify themselves as either hybrid or progressive firms. Of those firms, 49 percent classify themselves as hybrid firms offering an equal mix of advisory and compliance services, while 18 percent classify themselves as progressive firms offering substantial advisory services. The report also identifies expected advisory growth areas, including Virtual CFO and advisory work, cash flow forecasting, strategic planning, coaching, and ongoing accounting assistance. Moreover, many firms expect advisory services to represent a greater share of future revenue, with 14 percent anticipating that 70 percent or more of their next 12 months' revenue will come from advisory fees. A further 20 percent expect advisory services to generate more than 50 percent of future revenue. The areas identified for potential fee growth include Virtual CFO roles, strategic planning, and coaching.

Consumer preferences and expectations are changing, and consumers have come to expect the same level of convenience and service from all the entities with whom they interact. This trend is driven by advances in technology, increased digital access, and AI-enabled customer experiences. Digital disruption continues to reshape entire industries, forcing companies to adapt or risk obsolescence. Consider the fate of Blockbuster, a company that was unable to change with the times and compete with companies like Netflix. In contrast, companies like Kodak have pivoted their business model, evolving into technology-driven firms servicing sectors such as graphic arts, commercial print, publishing, packaging, and commercial entertainment.

Companies work hard to be creative with new products and services. However, it doesn't take long for those good ideas to be imitated due to digital connectivity, automation, and AI-enabled tools, resulting in a loss of competitive advantage to the company originating the idea.

Companies are relying on data to help them identify challenges in their operations, take advantage of opportunities, and make timely decisions. Increasingly, this includes using analytics and AI-assisted insights to recognize patterns, forecast outcomes, and respond more quickly to changing conditions.

[1] Spotlight Reporting's 2025/2026 Global Advisory Trends Report.

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.

A. Disruptive technologies

Finance and accounting professionals need to consider embracing continuous learning that goes past traditional continuing professional education. New digital competencies such as data literacy, process automation, AI-assisted analysis, and an understanding of generative AI and agentic AI are becoming essential for success in today's rapidly changing environment. The accounting industry faces imminent, sweeping disruption due to massive technological changes and evolving consumer trends, necessitating a fresh approach to value creation for clients. Some services, particularly basic transactional accounting, are more susceptible to disruption and have already seen significant automation, though adoption varies among small business types. Compliance and some limited advisory services are likely to become increasingly automated. In this evolving landscape, automated systems are expected to handle many routine tasks under professional oversight, allowing accounting professionals to shift their focus toward providing specialized insights, scenario-based guidance, and strategic advisory services that strengthen client relationships. These shifts are part of five key trends shaping the future of accounting.

During the initial stages of the generative artificial intelligence (GenAI) revolution, access to services like ChatGPT was mostly limited to specific websites or dedicated mobile apps. However, this approach is evolving. Leading technology companies are now integrating GenAI directly into widely used business applications, making AI functionality seamless. A prime example of this shift is Microsoft, the leading software provider for finance professionals. Through its Copilot suite, Microsoft is integrating AI-powered features into Excel, Outlook, Word, and Power Platform, enabling accountants and finance professionals to automate tasks, generate insights, and streamline workflows within the tools they already use. Similar AI-enabled capabilities are also being embedded across accounting, tax, audit, and practice management platforms. This deeper integration signals continued productivity gains for knowledge workers.

Accounting firms are increasingly seeking professionals with a digital mindset and strong technological fluency, those who can not only design inquiries and interpret results from advanced analytics but also act as trusted advisors in a data-driven world. As generative AI evolves toward more agentic capabilities, professionals will also need to understand how AI tools plan tasks, interact with systems, and produce outputs that require human review. However, as automation expands in audit and compliance services, some clients may expect a reduction in fees, not fully recognizing that the investment in tools and the complexity of oversight may actually increase. Later in this course, we will explore both the opportunities and risks posed by technologies such as data analytics, AI, and automation.

B. Drivers of change in a digital world

Multiple forces continue to shape the digital transformation of finance, and while technology is a major catalyst, it is not the only one. The following are four interconnected drivers of change that continue to shape today's digital world[2]:

[2] *Reinventing Finance for a Digital World*, CGMA, 2019.

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.
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 makes it doubly important to understand the patterns of behavior in the way people use technology, consume information, and make purchasing decisions.

II. Becoming a data-driven organization

Companies have increasing amounts of data in their systems that can provide insights to improve processes and performance. The problem is that it is not always the right data and when it is, it is not always utilized. Some companies may not want to make the investment to try to harness the power of the data. Others may make the effort only to have their executives guide the company by intuition.

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.

A. Key to digital transformation

The key to digital transformation is to become a data-driven organization, which requires a commitment and follow-through to using data to drive decision-making. This is easier said than done. The concept should be instilled not only in company leadership but in all employees. Managers and leaders should leverage data analytics and business intelligence (BI) tools to understand all aspects of the company's business, including hiring forecasts, supply chain, marketing, and finance. The challenge is not so much in the mechanics, because the technology is available and increasingly accessible, but in the organizational culture. Managers and leaders should also be challenging decisions that are made, asking what data was used to determine the decisions that were made. This requires courage and a commitment to transparency. Cultural resistance and overreliance on intuition are often where data-driven initiatives begin to break down.

B. Why this is important to finance and accounting

In the past, finance and accounting teams generally concerned themselves with budgeting and forecasting tools. Technological advances have now provided finance and accounting teams with the opportunity to use BI tools such as text analysis software, predictive analytics, natural language processing (NLP), AI-assisted analytics, and data preparation software to see relationships in the data that they were unable to see before and derive insights from the data to improve the company's performance.

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.

C. Data-driven decision-making

1. Benefits of data-driven decision-making

Data-driven decision-making offers numerous benefits, including providing a systematic approach rather than an erratic one, which facilitates the detection of opportunities and challenges. In environments characterized by significant market volatility and a dynamic funding landscape, it enables organizations to adapt swiftly and with agility. This method promotes an objective approach to decision-making, as opposed to a subjective one, and helps depersonalize the process, leading to greater standardization and consistency in decisions. Relying solely on intuition for decision-making can pose substantial risks.

Data-driven decision-making enables organizations to experiment with various strategies to determine their effectiveness. Decisions are made and progress is gauged using data rather than relying on emotional or instinctive judgments. This approach not only offers a predictive (forecasting future trends) rather than merely a historical perspective (analyzing past events) but also enhances confidence among decision-makers and stakeholders, as choices are founded on solid evidence rather than mere opinions. Furthermore, leveraging data from unconventional sources like social media or geolocation data and AI-

assisted forecasting tools enhances an organization's understanding of the preferences, needs, and concerns of its constituents.

2. Challenges and barriers with data-driven decision-making

As noted earlier, most companies function in a global business environment in one way or another. They are increasingly under immense pressure to make accurate and timely decisions. To do this, management needs to be able to identify opportunities as well as roadblocks and then adapt the entity to those changes. Even though many companies understand that data-driven decisions will help propel them towards this goal, they are not able to execute. Data-driven decision-making presents several challenges. Many organizations possess vast quantities of data but often do not effectively utilize it in their decision-making processes. Common barriers include poor data quality, decentralized systems, unclear data ownership, and limited data governance. Additionally, there is a growing demand for making swift, accurate decisions and delivering results promptly. Transitioning to a data-driven decision-making framework requires a significant shift in organizational culture and mindset. Frequently, employees may defer to the opinions of senior leaders rather than relying on data. Organizations are also faced with the dilemma of choosing between data-driven recommendations and the directives of their leaders. To navigate these challenges, staff at all levels must enhance their analytical skills and integrate data and analytical tools into their everyday tasks. As organizations adopt AI-enabled tools, they must also ensure the underlying data is reliable, secure, and appropriate for the intended use.

Earlier research[3] identified changes to decision-making processes and use of analytic and BI tools as well as some of the barriers to achieving a data-driven decision-making culture.

The chart below summarizes some of the cultural and cognitive barriers companies face when striving to become data-driven decision-making organizations.

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.
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.

[3] Harvard Business Review Analytic Services. *The Evolution of Decision Making: How Leading Organizations Are Adopting a Data-Driven Culture*. Sponsored by SAS. 2016.

Recency bias – A cognitive barrier	People use data points that are recent and do not always 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 actually may be more relevant, 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.
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.

These barriers can impede a data-driven organization's decision-making. However, there are solutions that can help to solve the issues that companies face.

Approach to mitigating the 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.
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, a company can hire people with the relevant skills 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.

D. Steps to become a more data-driven decision entity

As companies begin to change their decision-making processes there are a number of factors that they need to keep top of mind. Failure to implement these steps could result in wasted time and effort or analyses that do not really provide much insight into the problems they are trying to solve.

1. Decide what to measure

Companies can avoid wasted time and the expense associated with analysis by deciding what data are important to inform decision-making. Gathering data is really like any other business decision. Companies should evaluate the cost to collect and extract data. It may exceed the benefits.

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

2. Choose the correct BI Tools

There are numerous BI tools out there and management needs to consider the alternatives based on the size and complexity of the organization as well as the type of data that they want to collect. Excel has come a long way, but it is not robust enough for large data sets or complex analysis.

For big data analysis, a company will need to choose more sophisticated tools that will:

a. Provide robust data ingestion, integration, and preparation features;
b. Consume data through file uploads, database querying, and application connections;
c. Allow for modeling, blending, and discovery of data;
d. Create reports and visualizations with business utility;
e. Create and deploy internal analytics applications; and
f. Provide AI-enabled features, such as natural language queries, automated insights, or anomaly detection, where appropriate.

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.[4]

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

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

3. Identify the correct personnel to analyze data

Management will want to assign the 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. If there are not sufficient people already in the company, it is important to recruit and hire people with the talent and expertise to supplement existing staff.

4. Address the issue of decentralized data

Management will want to address the issue of decentralized data very early in the process. Most companies have systems that are siloed, and this makes data analysis more challenging. In some instances, it may take more effort to compile the data than to analyze it. Smaller companies may find that it is too expensive to fully integrate systems. However, they should look for ways to automate processes and analyze the most critical data while maintaining appropriate data governance, access controls, and data integrity.

When selecting a new system, companies should look toward systems able to fully integrate with existing systems.

5. Data security and data integrity

Data security refers to keeping data safe from unauthorized users and includes hardware solutions such as firewalls and software solutions such as multi-factor authentication and encryption. It is critical in preventing cyber-attacks. Data security is the fundamental general computer control. Data integrity builds on it 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. As a process, data integrity 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. If data lacks integrity, then it is useless to the analyst since the insights gained from analysis are then suspect. This becomes even more important when data is used in dashboards, automated workflows, or AI-enabled tools.

As data travels through a system, it must remain intact. Data can be damaged:

a. In transit from a computer to a storage device or over a network.
b. Hardware failures in storage devices or the computer itself can occur.
c. Software or security applications can be misconfigured resulting in damaged data.
d. 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.

Data integrity has several important aspects:

a. Data should have the time, date, and identity of those who recorded it.
b. Data should be in a standardized format and easy to read.
c. Data should be timely. Any time there is a delay in recording data there is an opportunity for loss.
d. Good data is maintained in its original format. It should be secured and backed up.
e. Data should be free of errors.

The system should have:

a. Controls to validate the input;
b. Controls to validate the data itself;
c. Controls to create backups;
d. Access controls; and
e. An audit trail.

6. 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. The keys to effective implementation of data-driven decision-making are open communication, training, enforcement of new policies and procedures, and responsible use of data and AI-enabled tools.

Technology Trends and Risks

Learning objectives 1
I. Top 10 technology trends 1
A. Cloud computing 1
B. Robotic process automation 2
C. Artificial intelligence 3
1. Traditional AI and machine learning 3
2. Generative AI and large language models (LLMs) 4
3. Agentic AI and autonomous tools 5
D. Advanced data analytics 5
1. Analytical procedures 6
2. Preliminary analytical procedures 7
3. Benford's Law 8
4. Substantive analytical procedures 11
5. Types of analytical procedures 12
6. Six-step method to perform an SAP 13
7. Example: Substantive analytical procedure – Case study 15
E. Integration of accounting and operations systems 18
F. Outsourcing the accounting function 19
G. Accounting and finance professionals will need different skill sets 19
H. Focus on transparency, objectivity, and validity – Blockchain 20
1. Blockchain and the audit process 22
I. Remote and hybrid accounting workflows 22
J. Changes in professional literature and internal control guidance 23
1. Committee of Sponsoring Organization (COSO) Framework 23
2. COSO Framework and three components related to IT controls 26
II. Top technology risks 28
A. Understanding where risk may be present 28
1. Reliance on systems that are inaccurately processing data or processing inaccurate data or both 28
2. Unauthorized access to data 29
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 29
4. Inappropriate changes could be made to systems or programs 29
5. IT personnel may make unauthorized or erroneous changes to data in master files 30
6. The entity may not make the necessary changes and updates to systems or programs 30
7. Potential loss of data or inability to access data as necessary 30
8. Risks introduced when using third-party service providers 31
III. Cybersecurity risks – Today's top cyber fraud schemes and how they work 33
A. Authorized push payment fraud (APP) 34
1. SMS spoofing 34
B. Deep fakes and voice biometrics 34
C. Breaching multi-factor authentication (MFA) 35
D. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks 35
1. TCP SYN flood attack 35
2. Teardrop attack 36
3. Smurf attack 36
4. Ping of death attack 37
5. Botnets 37
6. Ransomware and ransom attacks 37
E. Phishing and spear phishing attacks 38
F. Drive-by download attacks 38
G. Password attacks 38
H. Cross-site scripting attacks 39
I. Eavesdropping 39
J. Malware 40
K. Internet of Things (IoT) 40

L. It's also a people problem **41**
M. Statistics that are good to know **42**
IV. Internal control imperative ***43***
A. SEC cyber fraud report **43**
B. Internal controls to help prevent cyber fraud **44**
1. New section: Audit transformation *45*
C. Documentation **46**

Technology Trends and Risks

Learning objectives

Upon completing this chapter, the reader will 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.

I. Top 10 technology trends

In this dynamic environment, accountants in business and industry as well as those in public accounting firms need to understand where the technology focus is likely to be for the next 3 to 5 years. It is not a question of "if," it is a question of how quickly companies and accounting firms will begin to utilize the new technologies available to them. Like any change in business process, auditors will also need to understand the risks and control implications that new technologies bring to the audit.

This section will examine the top 10 technology trends:

1. Cloud Computing.
2. Robotic Process Automation.
3. Artificial Intelligence, including generative AI and agentic AI.
4. Advanced Data Analytics.
5. Integration of Accounting and Operations Systems.
6. Outsourcing 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.

A. Cloud computing

According to industry research by BlackLine, a digital finance transformation organization, almost 40 percent of CFOs globally express doubts about the accuracy of their organization's financial data. The survey, which involved over 1,300 C-suite and senior finance and accounting professionals from seven different markets (the United States, Canada, the United Kingdom, France, Germany, Australia, and Singapore), revealed that 37 percent of CFOs and about 50 percent of senior finance and accounting professionals do not fully trust their financial data.

Owen Ryan, co-CEO of BlackLine, emphasized the importance of data trustworthiness, stating, "Trusting the data organizations work with is critical for effective decision making, not only for the office of the CFO but for the entire business ecosystem." This trust is especially crucial in navigating unpredictable external events. The survey also highlighted widespread concern among respondents about various external threats: 78 percent are worried about another global financial crisis, 76 percent about the impact of cybersecurity issues, and 73 percent about new disruptive technologies affecting their business.

Additionally, the survey underscored ongoing concerns over financial visibility, with 98 percent of respondents indicating they do not have complete confidence in their organization's visibility over its cash

flow for the second year in a row. Furthermore, 37 percent of them acknowledged that real-time understanding of cash flow is essential for managing unforeseen market changes effectively.

Cloud-based accounting solutions are gaining in popularity. Companies are currently producing more and more data in the form of:

a. Transactional data;
b. 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
c. 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 is essentially outsourcing the processing of an entity's data to a network of remote servers hosted on the internet. It offers on-demand scalability, meaning both small and large entities can use it cost-effectively without investing in or maintaining expensive hardware. Cloud platforms also offer robust computational power, which is critical for executing advanced data analytics, running AI models, and accessing real-time financial dashboards.

Additionally, many platforms now offer cloud-native AI integrations, such as embedded machine learning models, anomaly detection, and natural language processing (NLP), that enable finance professionals to derive insights more efficiently from structured and unstructured data sources. As cloud adoption expands, organizations must also consider vendor risk, access controls, data governance, and security over cloud-based financial information.

B. Robotic process automation

Robotic process automation (RPA) mimics tasks that are performed by humans and automates them. It is used to handle high volume tasks that are repeatable such as making calculations or recording transactions. RPA is more consistent and accurate and can handle these tasks more quickly than a human can.

In **accounting and finance**, RPA is now widely used for automating:

a. Journal entries;
b. Bank reconciliations;
c. Invoice matching;
d. Extracting data from structured forms (e.g., PDFs); and
e. Uploading data between disconnected systems.

As RPA matures, it is increasingly integrated with artificial intelligence to create **intelligent automation (IA)** – the combination of rule-based logic and advanced technologies such as machine learning, natural language processing, and optical character recognition (OCR). In some organizations, these workflows are also beginning to incorporate agentic AI capabilities that can initiate, sequence, or adapt tasks with human oversight. This allows for semi-structured and even unstructured data to be incorporated into automated workflows.

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

a. Download a file;
b. Take certain data from the file;
c. Transfer that data to another file; and
d. 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 improved.

While RPA offers significant efficiency gains, its success depends on careful process selection, governance, and testing. Poorly scoped RPA projects can lead to:

a. Hidden errors if source systems change;
b. Inconsistent exception handling; and
c. Overdependence on a bot with no human review loop.

Auditors and controllers must consider how RPA impacts internal control design. Automated processes must be documented and monitored like any other critical system, and controls around inputs, outputs, and exception logs should be clearly defined.

C. Artificial intelligence

Artificial intelligence (AI) continues to transform the accounting profession by enhancing how professionals process information, make decisions, and deliver insights. From traditional machine learning to generative models and agentic AI, this evolution is reshaping workflows, expectations, and required skill sets.

1. Traditional AI and machine learning

AI can extract key information, generate content, automate tasks, and detect patterns or anomalies at scale. This trend has the most potential to change how finance, accounting and auditing professionals do their jobs. Algorithms are written that can evaluate large quantities of data and identify anomalies and risk, as well as find opportunities to enhance profitability. As with all emerging technologies, AI introduces questions about accuracy, reliability, and explainability. Users may want to understand how the system arrived at a specific result, yet this is not always possible, particularly when using complex models like large language models (LLMs), which do not follow transparent, auditable decision paths.

AI uses a logic and rules to form the instructions which are the basis of the algorithms. The most widely used application of AI is machine learning. Machine learning relies on the application learning to produce a more precise answer 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. 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 grouped into solving two types of problems: regression and classification. Regression problems are solved by prediction, and classification problems involve classifying input into categories such as whether a transaction is fraudulent or not.

Machine learning may be supervised, where the system is trained using labeled data (e.g., outcomes are known), or unsupervised, where the system looks for hidden patterns in unlabeled data.

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.

Unsupervised learning is commonly used in recommendation systems. For example, Amazon and Netflix use AI to analyze customer behavior and make personalized suggestions. In the audit space, unsupervised machine learning could be used to identify transactions that are not typical and may be the result of errors or fraud.

2. Generative AI and large language models (LLMs)

The next major evolution in AI is generative artificial intelligence (GenAI), including large language models like ChatGPT, Claude, Gemini, Copilot, and other AI assistants embedded in business applications. These models are trained on vast amounts of text and code and can generate written responses, analyze spreadsheet data, summarize regulations, and even simulate conversations.

Example: ChatGPT, one of the best-known GenAI tools developed by OpenAI, was trained on billions of words from online sources. This massive training set allows it to make complex associations and respond to user prompts with text, tables, summaries, or even basic code.

Since ChatGPT was introduced in November 2022, generative AI tools have found numerous uses in finance and accounting, including:

a. Drafting client emails or engagement letters;
b. Writing policy memos or summaries of tax guidance;
c. Creating visual dashboards with descriptive narratives;
d. Explaining complex financial topics for clients; and
e. Simulating “what-if” business scenarios.

The key to leveraging these tools effectively is rooted in prompt engineering, the ability to craft clear, specific instructions that yield useful outputs. Effective use also requires providing appropriate context, evaluating sources, and verifying outputs before relying on them. A poorly constructed prompt can produce incorrect or vague responses, whereas a well-crafted one can unlock the model’s full potential.

A recent study showed that prompt optimization techniques improved GPT’s performance on a CPA practice exam from a failing to a passing score. The improvement resulted not from changes to the model itself, but from how the questions were framed, illustrating that high-quality output depends heavily on the quality of the input.[1]

Prompt engineering does not require programming knowledge; rather, it calls for clear thinking, creativity, and iterative testing. LLMs can also be customized to respond in a specific style, tone, or format to meet user needs.

---

[1] Kenney, A. (2024, April 1). *GenAI for accountants: 10 prompt-writing tips*. Journal of Accountancy. Retrieved from https://www.journalofaccountancy.com/issues/2024/apr/genai-for-accountants-10-prompt-writing-tips.
Eulerich, M., Sanatizadeh, A., Vakilzadeh, H., & Wood, D. A. (2023). *Is it All Hype? ChatGPT’s Performance and Disruptive Potential in the Accounting and Auditing Industries*. SSRN. https://ssrn.com/abstract=4466326.

LLMs are designed to provide human-like responses. The quality of their answers improves as users refine their prompts and engage with the LLM, but professional judgment remains necessary when evaluating the output.

3. Agentic AI and autonomous tools

AI is progressing beyond content generation into agentic AI: systems that can autonomously plan, execute, and adapt to tasks using multiple tools and APIs. Unlike traditional generative AI tools that primarily respond to prompts, agentic AI can take multi-step actions, interact with software applications, retrieve information, update records, and initiate workflows. Examples include:

a. AutoGPT or BabyAGI-style tools that string together steps without user intervention;
b. AI copilots integrated into platforms like Microsoft Excel;
c. Chatbots that trigger automations, retrieve database info, or launch workflows; and
d. AI-enabled workflows that monitor transactions, draft analyses, prepare reconciliations, or route exceptions for review.

These tools promise dramatic efficiency gains, but they also introduce new risks related to data privacy, model bias, governance, auditability, access rights, and accountability. Because agentic AI may act across systems, organizations should establish clear guardrails, including human approval for higher-risk actions, role-based access, monitoring, audit trails, and procedures to stop or reverse inappropriate actions. Professionals must understand not only the capabilities but also the limitations and ethical boundaries of these tools, especially when using AI to support decisions that impact clients, stakeholders, or the public.

D. Advanced data analytics

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

Descriptive analytics – Provides insights into the past and helps the analyst determine what happened.

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 bad debts.

Diagnostic analytics – Involves the examination of data to answer why something may have happened.

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 discounts, instituted a policy change that allowed salespeople to give discounts of up to 15 percent without approval.

The auditor went back and performed a further analysis to determine if the percentage of 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.

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.

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 for 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.

Prescriptive analytics – Technique that builds on predictive analytics and answers the question, "How do we make it happen?"

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.

1. Analytical procedures

Auditors are required to perform analytical procedures in the planning stage of the audit as risk assessment procedures (AU-C 315). They are also required to perform analytical procedures in the final stages of the audit to assess the conclusions reached and evaluate the entity's overall financial statement presentation (AU-C 330). Auditors may find it beneficial to perform analytical procedures as substantive tests (AU-C 520). Substantive analytical procedures are usually performed on operating statement accounts.

SAS No. 145 mandates that firms understand how an entity uses technology relevant to the preparation of financial statements, influencing their audit planning by requiring tailored audit programs and procedures responsive to assessed risks. For instance, if a client implements new technology, firms cannot simply replicate previous audit processes as these may become obsolete. Instead, firms must thoroughly understand the new technologies to comprehend their impact on client workflows and adjust their audit procedures accordingly. Thus, SAS No. 145 creates opportunities for auditors to employ

technology in data analysis and innovate their auditing methods. One of the key advantages of incorporating technology and data analytics into auditing is the ability to overcome the limitations imposed by traditional sampling methods. Data analytics enables practitioners to examine large volumes of data, and in some cases entire populations, for anomalies, trends, and risk areas, providing a more comprehensive understanding of the data.

2. Preliminary analytical procedures

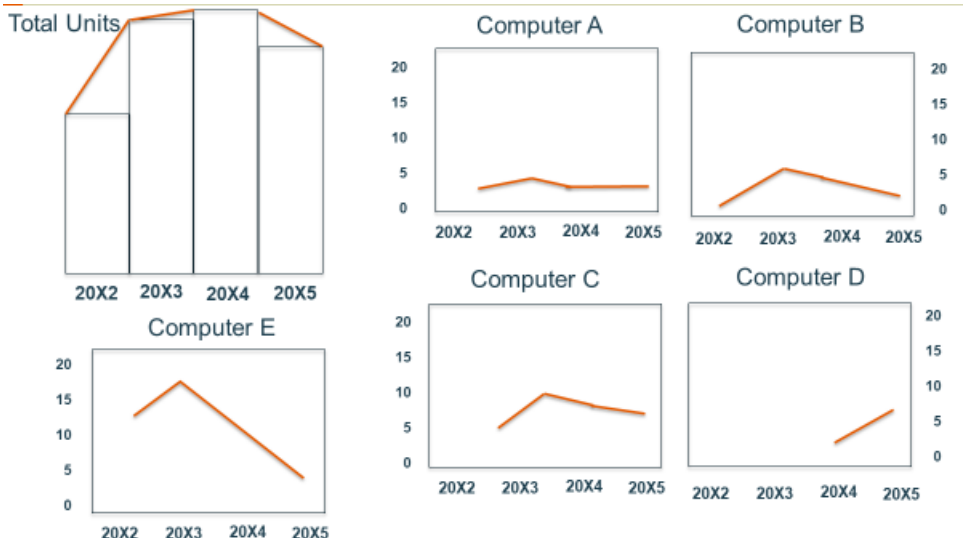
As preliminary procedures, data analytics can be performed at an aggregate level. They are intended to help the auditor understand where there are areas of risk in the audit. The auditor is required to develop an expectation based on information they have learned about the entity and its environment. The procedure itself usually takes the form of a fluctuation analysis or financial ratios. The auditor may find it helpful to go beyond just aggregate numbers for large accounts such as revenue, payroll, or other significant operating expenses. By using nonfinancial information and financial information together the auditor is able to drill down further into the risk. Auditors may also choose to perform other diagnostic analytics to assist the client in understanding where anomalies lie or as diagnostics to assess fraud risk. Presenting information in the form of a graphic is also informative. Modern data visualization tools can help auditors identify trends, outliers, and relationships that may warrant further investigation.

Examples of analyses that can be performed are:

a. Comparison of account balances with budget and prior-period amounts;
b. Analysis of changes in revenue during the current period based on statistical data;
c. Payroll expense divided by number of employees;
d. Other expense fluctuations from prior year; and
e. Relationship between the allowance for uncollectible receivables or pledges and revenue, aging categories, etc.

Example: An auditor was performing an analysis of revenue for computer sales by model type over a 4-year period. He wanted to understand why the number of computers sold in the current year was down when revenue was up. The data was easier to analyze once he put the information in graphical form. The auditor was able to see the total unit sales as well as the unit sales of the 5 different types of computers in the graphic below. The findings corroborated the client's assertion that the number of computers was down in total. The company was unable to obtain as many of Computer D, the highest priced model, from the manufacturer so there were fewer available to sell. The price of that model was driving the increase in sales dollars. Sales of computer E were expected to be down since the company was phasing it out. Sales of Computers B and C were down, and sales of Computer A were flat. Although the analysis enabled the auditor to explain the change in revenue it raised a question about inventory obsolescence.

This analysis was performed as a risk assessment procedure but was also used in the substantive analytical review of revenue.



3. Benford's Law

Benford's law is a theory about the distribution of digits in large data sets. It was developed in the 1920s by a man named Benford and has been the subject of research projects ever since. Appropriately constructed, it can detect anomalies in data for investigation. The distribution of numbers, according to the table shows that the number 1 would be the leading digit in a string of numbers 30.1 percent of the time. The number 2 would be the leading digit in a string of numbers 17.6 percent of the time. The table extends many placements out.

Example: An auditor was performing fraud interviews and was told that managers were splitting expense reports to approve expenses just under $500 limits. She decided to run a diagnostic to determine if that was likely before concluding it was a risk of fraud.

She ran a report of checks and tested the report for validity. The test showed the following:

Leading digit	Sample	Benford's Law
1	30.4%	30.1%
2	17.4%	17.6%
3	12.3%	12.5%
4	**14.8%**	**9.7%**
5	6.8%	7.9%
6	5.6%	6.7%
7	4.8%	5.8%
8	4.1%	5.1%
9	4.8%	4.6%

In examining and then graphing the numbers, it was clear to see that the place where the sample differed from Benford's law was the number 4. The auditor decided to investigate and found that the allegation was true.

Documentation

For preliminary analytical procedures, the auditor should document:

a. Plausible expectations;
b. Results of the procedures; and
c. Risks that emerge to be taken to the team meeting.

Note that preliminary analytics are not intended to serve as a substitute for planned audit procedures or substantive testing.

Example: ***Expectation:*** Based on discussions with management, review of the board minutes for the year and review of trends in the industry we have the following expectations. Based on discussions with management and review of sales reports provided by operations personnel we noted that sales of product were flat, and services decreased. We learned that there was some increased competition in the area from a larger company that sold at lower prices. We were able to corroborate this from external sources. Based on the review of the minutes we noted that the company replaced a piece of equipment that was old for $6,500. In addition, we know from discussions with management that there were significant issues with their billing system and, as such, bills for the last few months did not go out as scheduled. We corroborated this by reviewing the AR run that took place shortly before year end. This accounts for the significant difference in accounts receivable. Accounts payable and cash typically fluctuate due to timing and so we do not expect that any fluctuations +/- $25,000 would be unusual. In 20X8 the company wrote off a significant amount of inventory due to some damage sustained to the warehouse. Margin appears consistent and inventory did not decrease from 20X8 to 20X9. We will follow up on this issue as it appears to be a risk. The only fluctuation, aside from inventory that is unexplained, is other assets. The amount is not significant and so although we will follow up on this during our substantive testing, it does not appear to be a significant risk or risk of fraud. We will carry forward the risk associated with inventory to be considered in the team discussion.

Balance Sheets

	20X9	20X8	$ Change 20X9-20X8	% Change 20X9-20X8
Assets				
Current assets:				
Cash and cash equivalents	$ 312,833	$ 469,633	$ (156,800)	-33.39%
Accounts receivable	712,625	521,000	191,625	36.78%
Related party receivable	2,953	3,542	(589)	-16.63%
Inventory	655,000	650,162	4,838	0.74%
Other assets	19,633	310	19,323	6233.23%
Total current assets	1,703,044	1,644,647	58,397	3.55%
Property and equipment:				
Office furniture, equipment and software	179,039	172,394	6,645	3.85%
Less accumulated depreciation	93,101	86,103	6,998	8.13%
Property and equipment, net	85,938	86,291	(353)	-0.41%
Other assets:				
Investments	53,456	48,452	5,004	10.33%
Total other assets	53,456	48,452	5,004	10.33%
TOTAL ASSETS	$1,842,438	$1,779,390	$ 63,048	3.54%
Liabilities and Retained Earnings				
Current liabilities:				
Accounts payable				
Trade	$ 40,546	$ 69,545	(28,999)	-41.70%
Other	8,505	8,897	(392)	-4.41%
Accrued payroll and payroll related liabilities	91,856	$ 69,899	21,957	31.41%
Deferred revenue	53,508	45,279	8,229	18.17%
Total current liabilities	194,415	193,620	795	0.41%
Notes Payable	1,298,258	1,360,238	(61,980)	-4.56%
Total Liabilities	1,492,673	1,553,858	(61,185)	-3.94%
Common Stock	1,000	1,000	-	0.00%
Retained earnings	348,765	224,532	124,233	55.33%
Total Shareholder's Equity	349,765	225,532	124,233	55.08%
TOTAL LIABILITIES AND SHAREHOLDER'S EQUITY	$ 1,842,438	$ 1,779,390	$ 63,048	-

Statements of Operations				
	20X9	20X8	$ Change 20X9-20X8	% Change 20X9-20X8
Revenue:				
Product Sales	$ 1,184,327	$ 1,174,814	$ 9,513	0.81%
Service contracts	289,275	337,483	(48,208)	-14.28%
Investment income	8,275	7,806	469	6.01%
Total revenue	1,481,877	1,520,103	(38,226)	-2.51%
Expenses:				
Payroll and benefits	238,406	254,873	(16,467)	-6.46%
Cost of product sold	1,045,395	1,050,021	(4,626)	-0.44%
Administrative expenses	58,652	51,459	7,193	13.98%
Total expenses	1,342,453	1,356,353	(13,900)	-1.02%
Pretax income	139,424	163,750	(24,326)	-1%
Income tax expense	(14,530)	(16,550)	2,020	-12.21%
Net income	124,233	147,200	(22,967)	-15.60%

Supplemental analytics - Revenue

Product Sales	$ 1,184,327	$ 1,174,814	$ 9,513	0.81%
Cost of product sold	(1,045,395)	(1,050,021)	4,626	-0.44%
Margin	138,932	124,793	14,139	11.33%
Margin %	12%	11%		

Service contracts	$ 289,275	$ 337,483	(48,208)	-14.28%
Number of customers served	175	205	(30)	-14.63%
Average Revenue per contract	$ 1,653	$ 1,646	7	0.41%

4. Substantive analytical procedures

The auditor must perform substantive procedures for all significant account balances and classes of transactions. Vouching, confirmation, and other tests of details can be performed along with substantive analytical procedures. The auditor may choose to perform one type of procedure or may choose a combination of procedures within constraints.

Risk Assessment	Testing Combinations
Significant risk	• Tests of details alone. • SAP combined with tests of details. • SAP combined with tests of controls.
Not significant risk	• Tests of details alone. • Substantive analytical procedures alone. • Combination including tests of controls, but it is not possible to simply perform tests of controls.

Substantive analytical procedures (SAP) help the auditor to better understand the business. But they are not always the best procedure to choose. The auditor should ask the following:

a. Given the assertions to be tested, how suitable is an SAP?
b. How reliable is the data that will be used to develop the expectation?
c. Will the expectation be sufficiently precise at the desired level of assurance?
d. What is the amount of unexplained difference that will be acceptable to the auditor?
e. What is the risk that management could override controls so that an adjustment made outside the normal period end financial reporting process could have been made and alter the auditor's conclusions?

Where preliminary analytical procedures were not required to be performed at a disaggregated level, it would be difficult to perform SAPs any other way and achieve the necessary precision. Precision is defined as a measure of the closeness of the expectation to the recorded amount. If SAPs are going to produce the primary evidence for the account balance or class of transaction, then precision should be high. AU-C 520 states that tolerable misstatement should be the guide.

Certain balances are easy to predict. For example, there are limited variables in interest expense, even when there are multiple debt issues. Revenue, on the other hand, is more challenging because of the number of products or services and prices involved. As noted in the section on evidence, when using information from reports, the reports will need to be tested to ensure that the content of those reports is reliable.

There are six steps to performing an SAP:

1. Form the expectation.
2. Set a threshold for unexplained differences (precision).
3. Compare the expectation to recorded amounts.
4. Investigate differences between the expectation and recorded amounts that exceed the desired threshold.
5. If reasonable, supportable explanations cannot be obtained and corroborated by other evidence for amounts over the threshold, the auditor may choose to disaggregate the balance further. The auditor may also choose to test a portion of it by SAP and another portion by tests of details.
6. Where the auditor is unable to substantiate the unexplained differences over the threshold and they do not wish to perform other substantive tests, they must consider the effects both individually and in the aggregate of misstatements (known and likely) that are not corrected by the entity.

5. Types of analytical procedures

Method	How it works	Precision
Trend analysis	Compare current year to prior year(s)	• Less precise than other forms, more appropriate for preliminary analytical procedures. • Using one year can lead to bias unless it can be substantiated that the environment is stable. • Can only factor in one variable.
Ratio analysis	Comparison of relationships between financial statement accounts between two periods or over time. This can be the comparison of an account with nonfinancial data or comparison between relationships between financial data and industry stats	• This method only works when relationships are stable. It is important to disaggregate data. • Can only factor in one variable.

Reasonableness or predictive expectation. Very explicit	Takes into consideration the auditor's knowledge of the business and industry	More precise because the auditor can factor in more than one variable
Regression analysis	Uses the relationship between dependent and independent variable(s) to develop an expectation and evaluate the strength of that relationship	Provides direct, quantitative measure of the precision of the expectation. R-squared, T statistic, and standard error of the estimate

Trend and ratio analysis are appropriate for preliminary analytical procedures and for supplementary SAPs but will generally not be sufficiently precise for a primary substantive test. Predictive tests and regression analysis are generally used as substantive tests.

6. Six-step method to perform an SAP

The six steps in performing an SAP follow.

Step 1: Form the expectation.

To successfully perform an SAP, the auditor needs a good understanding of the account balance or class of transaction being tested. Certain types of accounts lend themselves to effective SAPs more than others.

a. Balance sheet accounts can be tested with SAPs, but it is generally more difficult because balance sheet accounts represent amounts at a point in time. Classes of transactions make better SAP candidates because the transactions are over a period of time.

b. The assertion to be tested is also important to consider. SAPs are good procedures for testing estimates (valuation). SAPs are also good procedures for testing occurrence.

Account balances/classes of transactions will generally need to be disaggregated for a more precise expectation. Even then, it may be necessary to remove components of an account balance and test the details if there are too many variables to make a precise enough estimate for the entire balance.

In a smaller company, expenses could be separated into categories such as payroll, contractual items, and operating items adjusted for inflation or circumstance. For accounts that do not have significant types of changes from year to year, such as payroll expense, it may work well to use the prior year balance and then modify the prior year balances for additions, terminations, raises, and bonuses. It is important to understand the business drivers in order to get relevant data for the expectation.

The auditor needs to evaluate the **reliability** of the data used in the expectation considering the following:

a. Systems with reliable controls generally produce more reliable expectations.
b. Use external data for a more reliable expectation.
c. Nonfinancial data or data subjected to auditing procedures produces a more reliable expectation (attribute testing of accumulation of information).
d. Testing internal controls should be considered.
e. Industry trends are helpful but won't generally produce a precise enough result. They work better for preliminary or supplementary analytical procedures.

Step 2: Set a threshold for unexplained differences (precision).

The auditor should consider the difference that will be acceptable without further investigation. This is referred to as precision. The threshold for unexplained differences must be set low enough so that the auditor will have sufficient evidence to conclude that the financial statements are not materially misstated. As noted earlier, AU-C 520 says that precision should be guided by tolerable misstatement.

Step 3: Compare the expectation to recorded amounts.

Once the auditor performs the procedure, they will compare the expectation to recorded amounts. Differences from expectation can be due to:

a. Misstatements;
b. Inherent factors that affect the account being audited; and
c. Differences due to factors related to the reliability or completeness of the data.

The greater the precision of the expectation, the more likely it is that variances between the expectation and actual are due to misstatements. If the auditor does not believe the test will be sufficiently precise, then they should choose another type of test. Although the literature does not give precise numeric guidelines, if controls are tested and found reliable, there is more margin for acceptable difference. If controls were found to be moderately reliable or unreliable, then the threshold could be proportionately less.

Step 4: Investigate differences over the threshold.

The auditor performs SAPs realizing that the expectation is unlikely to equal the recorded balance. If the amount is over the threshold, then the auditor will need to investigate the unexplained difference. First, the auditor asks management to see if some business driver has been omitted. It is important to note that corroborative inquiry alone is not sufficient. The auditor will need to substantiate management's explanations.

Step 5: If reasonable, supportable explanations cannot be obtained and corroborated by other evidence for amounts over the threshold, the auditor may choose to disaggregate the balance further. The auditor may also choose to test a portion of it by SAP and another portion by tests of details.

Step 6: Where the auditor is unable to substantiate the unexplained differences over the threshold, and they do not wish to perform other substantive tests, they must consider the effects both individually and in the aggregate of misstatements (known and likely) that are not corrected by the entity.

7. Example: Substantive analytical procedure – Case study

An auditor decided to perform an SAP on revenue for a convenience store. The client was a convenience store chain with 15 stores. Some of the convenience stores sold gas and some did not. This was a driver of sales. Some were in favorable locations. Based on knowledge of the client, the auditor knew that revenue was usually stable unless a new product or service was introduced. In past years, the introduction of check cashing services and sales of lottery tickets made a difference.

Following is the data that the auditor collected.

Store Number	Prior Year Sales (audited) dollars	Current Year Sales dollars	Dollar change	Percentage change	Square feet	Average FTE	Inventory	Comments	Sells Gas (Y,N)
1	NA	864,225	864,225	NA	2,450	11.00	48,762	NEW & FAVORABLE	N
2	1,168,285	1,154,850	(13,435)	-1.150%	2,450	11.50	44,292		N
3	1,147,534	1,199,173	51,639	4.500%	2,450	12.50	45,841		N
4	NA	903,554	903,554	NA	4,200	11.80	38,120	NEW & FAVORABLE	N
5	2,037,528	1,991,480	(46,048)	-2.260%	4,200	10.90	46,225		**Y**
6	2,295,451	2,338,835	43,384	1.890%	4,200	11.34	53,864	FAVORABLE	**Y**
7	1,847,652	1,926,732	79,080	4.280%	4,200	10.73	50,903		**Y**
8	1,926,548	1,827,523	(99,025)	-5.140%	4,200	7.52	47,175	FAVORABLE	**Y**
9	1,845,931	1,836,332	(9,599)	-0.520%	4,200	14.25	60,915	FAVORABLE	N
10	NA	775,620	775,620	NA	2,500	11.25	34,502	NEW	N
11	984,218	1,182,154	(197,936)	-20.111%	2,500	11.56	18,775	FAVORABLE	N
12	1,068,478	1,143,271	(74,793)	-7.000%	2,500	12.75	34,652		N
13	NA	948,520	948,520	NA	4,200	11.81	45,182	NEW & FAVORABLE	N
14	1,805,100	1,991,025	(185,925)	-10.300%	4,200	12.25	38,757		**Y**
15	2,165,997	2,350,757	(184,760)	-8.530%	4,200	11.20	55,436	FAVORABLE	**Y**
	18,292,722	22,434,051	2,854,500	(0)	52,650	172	663,401		

The auditor tested the internal controls over sales and reconciled the amounts to the general ledger. The data was provided by the sales department.

Preliminary analytical procedures

The auditor performed preliminary analytical procedures at an aggregate level for all account balances and classes of transactions. As a further risk assessment procedure, they performed the analytics specifically on sales and used the data for those procedures as well as later during the audit for substantive testing. Based on knowledge of the business, reading of the minutes, and other inquiries, the auditor developed their expectation assuming:

a. No significant events or accounting changes occurred except store openings;
b. Industry and economic factors are stable; and
c. Materiality is $220,000 and tolerable misstatement is $165,000.

The auditor's expectation was that sales would not fluctuate in the aggregate except due to the sales for the four stores that opened during the year. The economy was flat so same-store sales were not expected to fluctuate more than 1 or 2 percent.

	Current Year	Prior Year	Change	Percentage Change
Total Sales	22,434,051	18,292,722	4,141,329	22.64%
Amount of sales for stores opened part of the year			3,491,919	
Same store sales	18,942,132	18,292,722	649,410	3.55%

At an aggregate level, the auditor determined that the fluctuation was higher than expected but decided that it was not a high enough difference to pose a significant risk. Next the auditor performed another analysis related to gross margin to see if there were any issues that needed to be identified as risks.

	Current Year	Prior Year
Total Sales	22,434,051	18,292,722
Cost of goods sold	15,423,410	13,234,784
Gross Margin	7,010,641	5,057,938
Gross Margin Percentage	**31.25%**	**27.65%**
Stores that sell gas (5,6,7,8,14,15)		
Sales	12,426,352	12,078,276
Cost of goods sold	8,431,280	8,439,091
Gross Margin	3,995,072	3,639,185
Gross Margin Percentage	**32.15%**	**30.13%**
Stores that do not sell gas		
Sales	10,007,699	6,214,446
Cost of goods sold	7,065,436	4,841,053
Gross Margin	2,942,264	1,373,393
Gross Margin Percentage	**29.40%**	**22.10%**

a. The auditor expected a higher gross margin for those stores selling gasoline. (TEST EXPECTATION MET.)
b. The gross margin should be more consistent for the stores that sell gas than those that do not. (TEST EXPECTATION MET.)
c. The margin for the stores that do not sell gas fluctuates more than the ones that do. This is because those that do not sell gas have a larger proportion of other inventory. In the current year, the company negotiated a favorable supply contract, and this increased the margin for products other than gas.
d. The auditor considered materiality ($220,000) and concluded that although this test was not precise enough to be a substantive test, it was useful in helping to identify that the differences that were noted in the analysis did not point to the presence of significant risks.

Substantive analytical procedures

The auditor decided to use an industry statistic to refine the expectation for sales. Management's goal was to achieve the average dollar sales per square foot according to the statistics put out by the National Association of Convenience Stores (NACS). The amount for 20X3 was $485 per square foot. The auditor knew that the new stores were not open for an entire year, so this statistic was first used to predict same store sales.

Store Number	Current Year Sales Dollars	Square Feet	Average per Square Foot in Dollars	Average per Square Foot (NACS) in Dollars	Difference	Percentage Difference	Sales for Stores Opened part of year	Sq feet for Stores Opened part of year
1	864,225	2,450	352.74	485	(132.26)	-27.27%	864,225	2,450
2	1,154,850	2,450	471.37	485	(13.63)	-2.81%		
3	1,199,173	2,450	489.46	485	4.46	0.92%		
4	903,554	4,200	215.13	485	(269.87)	-55.64%	903,554	4,200
5	1,991,480	4,200	474.16	485	(10.84)	-2.23%		
6	2,338,835	4,200	556.87	485	71.87	14.82%		
7	1,926,732	4,200	458.75	485	(26.25)	-5.41%		
8	1,827,523	4,200	435.12	485	(49.88)	-10.28%		
9	1,836,332	4,200	437.22	485	(47.78)	-9.85%		
10	775,620	2,500	310.25	485	(174.75)	-36.03%	775,620	2,500
11	1,182,154	2,500	472.86	485	(12.14)	-2.50%		
12	1,143,271	2,500	457.31	485	(27.69)	-5.71%		
13	948,520	4,200	225.84	485	(259.16)	-53.44%	948,520	4,200
14	1,991,025	4,200	474.05	485	(10.95)	-2.26%		
15	2,350,757	4,200	559.70	485	74.70	15.40%		
	22,434,051	52,650	6,391	485	(884)	-12.2%	3,491,919	13,350

Testing the same store sales

NACS statistic – Sales per square foot		485
	Sales	**Square Footage**
Totals for year	22,434,051	52,650
Less sales and SQ FT for stores opened part of the year	3,491,919	13,350
Sales for stores open all year	8,942,132	39,300
Times NACS Average		485
Expected sales for stores open all year		19,060,500
Difference between expected and actual		(118,368)
Percentage difference		-0.6210%

The auditor met the expectation with this test. The difference between actual sales per square foot and predicted was $118,368 in total. That was less than 1 percent. In addition, it was approximately half of materiality. The test was sufficiently precise, and the test expectation was met.

Testing new store sales

The new stores still needed to be analytically reviewed. First the auditor used the NACS statistic. The difference was too high even after adjusting that statistic for the 7 months (average) that the stores were open.

	Current Year	Square Ft
Total Sales New stores	3,491,919	13,350
Amount of sales per sq ft NACS		485
Amount projected for 12 months		6,474,750
Stores opened average of 7 months	3,776,938	3,776,938
Difference	(285,019)	

To refine the test the auditor took sales per store and performed the test disaggregating the stores.

Store Number	Current Year Sales Dollars	Square Feet	Average per Square Foot in Dollars	Average per Square Foot (NACS) in Dollars	Number of months open	Adjusted NACS per Sq Ft	Difference	Percentage Difference	INVESTIGATE
1	864,225	2,450	352.74	485	6.00	242.50	110.24	22.73%	YES
4	903,554	4,200	215.13	485	5.00	202.08	13.05	2.69%	
10	775,620	2,500	310.25	485	8.00	323.33	-13.09	-2.70%	
13	948,520	4,200	225.84	485	9.00	363.75	-137.91	-28.44%	YES
	3,491,919	3,338	276	485	7.00	282.92	(27.70)	-1.43%	

The auditor was able to determine that there were two stores that could be considered reasonable, but two could not. Stores 1 and 13 needed further work. The auditor considered their next steps.

Discussion questions:

a. Do you believe that the analysis for the existing stores is sufficient to conclude that the test expectation was met?
b. What follow-up do you believe the auditor should perform on the new stores?
c. What tests would you perform to ensure the reliability of the data?

E. 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. This is increasingly important as organizations seek clean, connected data for dashboards, automation, and AI-enabled analysis.

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. The 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. An ERP system 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.

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 where the ERP system has a lot more components such as human resources, inventory management, sales and distribution, 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.

F. Outsourcing the accounting function

Some businesses are outsourcing their entire accounting functions to third parties so they can concentrate on operations. According to industry analysts, the global business process outsourcing (BPO) sector continues to grow steadily, driven in part by demand for finance and accounting services enhanced with AI and automation. Outsourcing providers often benefit from economies of scale and may operate in lower-cost regions or leverage cloud-based technologies to reduce infrastructure burdens for clients. By outsourcing the accounting function, an entity can avoid investing directly in software systems that require continual maintenance and upgrades, especially complex ERP and compliance platforms.

In recent years, a growing number of firms have embraced Virtual CFO (vCFO) services, which combine outsourced financial reporting, forecasting, and strategic advisory. Some of these services are human-led, while others use AI-augmented platforms to provide dashboarding, alerts, and even automated financial insights. Outsourcing and offshore teams are also increasingly used to expand capacity, reduce compliance bottlenecks, and allow accounting professionals to spend more time on client-facing advisory work.

However, outsourcing does come with notable risks. Data security, quality of service, and geopolitical instability in some service regions can introduce exposure. In particular, data breaches or poor-quality financial reporting can affect not only operations but also compliance and audit readiness. Where AI-augmented services are involved, organizations should also understand how outputs are reviewed, who is responsible for exceptions, and how automated processes are monitored.

Quality assurance and strong internal controls over financial reporting (ICFR) should be of prime concern when evaluating any outsourced accounting provider. Organizations must assess the service provider's cybersecurity posture, staffing model, and alignment with industry standards for security and internal controls, such as SOC 1 and SOC 2 reports, as well as ISO 27001 certification, to ensure outsourced services do not create downstream risks.

G. Accounting and finance professionals will need different skill sets

The biggest challenge that companies and accounting firms will face going forward is that employees, particularly those 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 analytic 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.

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. 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 analytic skills. Public accounting firms may find it is easier to identify current employees with an aptitude and help them improve in the areas needed, including data analytics, automation, and AI-enabled tools.

As a client's IT system becomes more integrated and the technologies the client employs 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 modern system architecture and the development lifecycle for emerging technologies. Traditional audit team members may not have deep expertise in IT. Accordingly, it may be difficult for them to develop an adequate understanding of the design and implementation of these controls. In addition, if information is only available in electronic form, which is a trend, controls will need to be tested. The audit team should determine whether individuals with specialized skills, such as IT auditors, data specialists, or AI governance specialists, are needed to perform this work.

H. Focus on transparency, objectivity, and validity – Blockchain

One type of technology that promotes the notion of transparency, objectivity, and validity is blockchain. 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[2] 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?" 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 is immutable (can't be changed) because it is decentralized. In other words, the digital information is distributed and since no one entity controls or maintains it, it cannot be copied or altered by others. Each entity on the blockchain would need to be attacked simultaneously in most instances for an unauthorized alteration to occur. And for public blockchains, since anyone can join the chain 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.

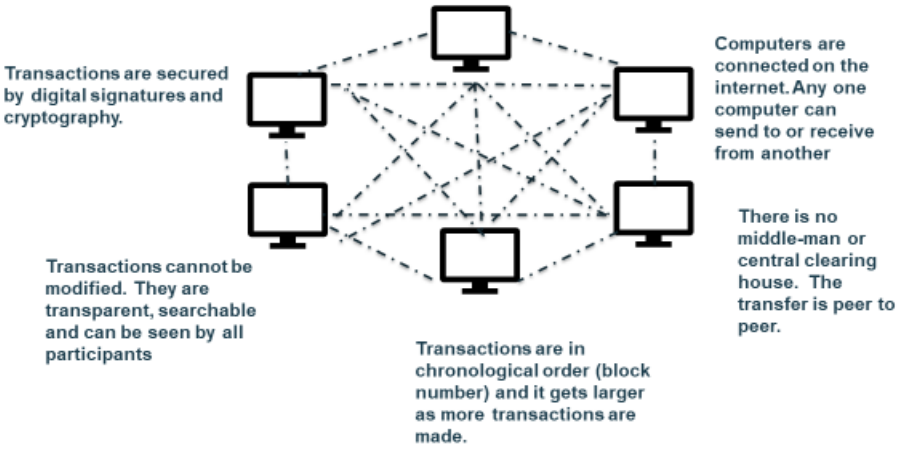
---

[2] *Elliott, Francis; Duncan, Gary (3 January 2009).* "Chancellor Alistair Darling on brink of second bailout for banks." *The Times*. Retrieved 27 April 2018.

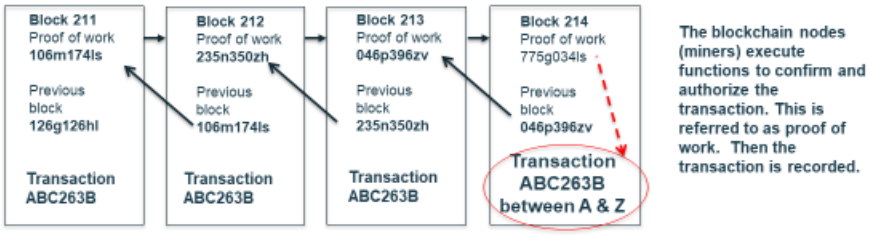
The “block” is a record of a new transaction and when it has been verified it is added to the chain. If an individual or company owns bitcoin, they have a key (password) to an address on the chain and that is where their ownership is recorded. There is no centralized processing entity (middleman) needed for these transactions who would likely take a percentage of the transaction as a fee.

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). The example below was adapted from a Deloitte article, *Blockchain: A Game Changer for Audit Processes*.[3]

Blockchain-Simplified Illustration 1/2



Blockchain – Simplified Illustration 2/2



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 block chain 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.

[3] https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html.

Blockchain is strongly associated with virtual currencies, but it could be used for many types of transactions and record keeping. Contracts could be embedded in virtual code and stored in distributed databases that are protected from deletion, tampering, and revision. A Harvard Business Review article, *The Truth about Blockchain*, suggests that at some point, attorneys, brokers, and bankers could become obsolete.

1. Blockchain and the audit process

A blockchain serves as an open ledger, independently verified between two parties that cannot be altered. This means that it could be used as a source of verification for reported transactions. Instead of sending confirmations to third parties the auditor can confirm with the blockchain. This would enhance audit coverage in a major way. Since blockchain is almost "real time" a continuous audit could be performed, assuming the auditing standards evolved to match the technology. Blockchain, however, is not without hazards. In 2022, threat actors stole approximately $3.8 billion in digital currencies (i.e., cryptocurrencies) according to a report by Chainanalysis. The thefts were typically not of the blockchain per se, but with the currency wallets and computers of the parties to the blockchain. These thefts illustrate 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.

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.

I. Remote and hybrid accounting workflows

With the widespread adoption of cloud computing and the growing reliance on electronic documentation, accountants are now more able than ever to work remotely or in hybrid environments. What was once a gradual shift toward remote audits has now become common practice, particularly among mid-sized and large firms.

Audit and assurance engagements now routinely rely on:

a. Cloud-based audit platforms;
b. Secure digital evidence repositories;
c. Remote collaboration tools; and
d. AI-enhanced document review and confirmation systems.

These tools enable accounting professionals to:

a. Request, receive, and evaluate client-provided documentation securely;
b. Perform real-time reviews from distributed locations; and
c. Maintain audit trails and data integrity without needing physical proximity.

However, remote workflows also introduce new risks, including:

a. Secure access to client systems;
b. Authentication and identity management;
c. Control over digital-only evidence; and
d. Appropriate use and review of AI-assisted tools in remote audit workflows.

As remote and hybrid workflows become the norm, accounting professionals must stay fluent in using mobile-enabled platforms, collaboration software, and remote assurance techniques, while adhering to the same level of professional skepticism and data governance as traditional engagements.

J. Changes in professional literature and internal control guidance

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. The 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.

1. Committee of Sponsoring Organization (COSO) Framework

The most prevalent framework used for internal control over financial reporting is the COSO framework. There are five elements of internal control identified in the framework: (i) the control environment; (ii) risk assessment process; (iii) control activities; (iv) information and communication; and (v) monitoring. For purposes of this course, we will discuss the two that have a significant impact on the financial reporting system regarding IT.

a. **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). Regarding the risk assessment element as it addresses IT, management should consider the following:

(i) The entity identifies risks to achieving its objectives and analyzes risks to determine how the risks should be managed; and

(ii) 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.

Example: ***Using a Risk and Controls Matrix to Map Risks to Control Activities***

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).

Following is an excerpt of one EPF control and risk process description and matrix.

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

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

(iii) 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.

(iv) 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.

(v) The entity identifies and assesses changes that could significantly impact the system of internal control.

(vi) 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.).

b. **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.

To begin, the auditor 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. The auditor should consider:

(i) New revenue streams;
(ii) Changes in the roles and responsibilities of entity personnel;
(iii) Automation of manual tasks;
(iv) Changes in staffing levels;
(v) Changes in the way that the entity's systems are developed and maintained; and
(vi) How well the design and implementation of general computer controls addresses identified risks.

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:

(i) Direct and indirect effects of the new technology and how it impacts audit risk;
(ii) How technologies impact the flow of transactions; and
(iii) The appropriateness of management's processes to select, develop, operate, and maintain controls related to the entity's IT.

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.

c. **Information and communication** – The fourth element of the COSO's Integrated Internal Control Framework is information and communication. The COSO Framework includes three components related to IT controls.

2. COSO Framework and three components related to IT controls

The COSO Framework includes the following three components related to IT controls.

a. **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.

Applications may be the general ledger system and its various interfacing modules such as accounts receivable, accounts payable or payroll or non-interfacing systems such as fixed asset packages or other systems that process information that ends up in financial statements.

Application controls can be programmed; that is, contained in the computer program, or manual that is performed by a person. 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.

Overall control objectives of any IT application are to ensure:

(i) Complete, accurate, valid data; and
(ii) Output that is distributed to authorized users.

There are four broad types of application controls that are used to achieve the internal control objectives of the various cycles. They are:

(i) **Input controls** – These controls are designed to ensure that the data entered into the system is complete and accurate.

(ii) **Processing controls** – These controls are designed to ensure that data is processed completely and accurately, and data integrity is maintained while processing and in storage.

(iii) **Output controls** – These controls are designed to ensure that reports produced by the system are distributed to only authorized personnel.

(iv) **Security controls** – These controls are designed to ensure that data stored and processed by the application are protected from unauthorized access, modification, or loss.

A comprehensive discussion of application controls is beyond the scope of this course. For more information, *IT Control Objectives for Sarbanes-Oxley,* an ISACA publication can be found at http://www.isaca.org.

b. **General Computer Controls** – General computer controls are broad and include controls over:

(i) Access/identity and access management;

(ii) Change and incident management;

(iii) Systems development;

(iv) Data backup and recovery; and

(v) Physical security that is related to the integrity of financial reporting processes.

They contribute to the overall reliability of the information technology and are not related to a specific application. With many smaller entities, access control is often lacking. Lack of access controls should be evaluated to determine how serious a deficiency it is. Often, 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:

(i) Vendors can access the system only for a short period after installation;

(ii) Terminated employees no longer have access to the system; and

(iii) When job responsibilities are changed, access to data is also changed.

c. **End User Computing** – End user computing includes the use of spreadsheets and other user-developed programs (such as databases) and involves:

(i) Documentation of these programs;

(ii) Program security;

(iii) Back up; and

(iv) Regular review for processing integrity.

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. However, the auditor should determine that:

(i) System updates were properly installed; and

(ii) New applications were tested and are running properly.

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.

II. Top technology risks

As companies embrace new technologies, they can expect to reap significant benefits. However, changes to any system should be evaluated to see where risk is present and where additional controls may be necessary. This list of the top technology risks is outlined in PCAOB AS 2110, *Identifying and Assessing Risks of Material Misstatement*.

A. Understanding where risk may be present

Management and their auditors should understand the risks that may be present due to specific programs or applications being introduced in the financial reporting system that are different from traditional systems. To do this they should obtain sufficient knowledge of the information system, including the related business process relevant to financial reporting to understand:

a. Procedures used to initiate, authorize, record, process and report information in the financial statements whether automated or manual;
b. Related accounting records, whether electronic or manual, supporting information and specific accounts in the financial statements;
c. How the information system captures events and conditions, other than classes of transactions that are routinely processed;
d. Processes used to prepare the entity's financial statements, including significant accounting estimates and disclosures;
e. Procedures and technology such as firewalls used to safeguard the entity's data; and
f. Extent of cybersecurity and access controls.

In developing the understanding management and their auditors should also understand what can go wrong and determine if the entity's internal controls are sufficient to address the relevant risks. Following are the top risks that should be evaluated and addressed as discussed in PCAOB AS 2110.B4.

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.

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 errors 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

This is a risk of both error and fraud. A person could destroy data, make inappropriate changes to data, or record fictitious transactions. If multiple users have access to a common database, it may be difficult to tell where the alteration originated.

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, multifactor authentication, password policies, access reviews, and other identity and access management controls.

Example: **Configuring the IT Infrastructure to Support Restricted Access and Segregation of Duties**

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:

a. Rate each application on its importance to financial reporting reliability;
b. Specify security policies for each rating level;
c. Assign each application a risk rating relating to its impact on financial reporting reliability; and
d. 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 and remains consistent with the principle of least privilege.

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.

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 at regarding internal controls is the AICPA Trust Principles, which are used in establishing criteria for service organizations.

There are three principles related to data availability:

a. **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.

b. **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.

c. **A1.3:** The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Following are example controls that could be implemented that would be responsible to the principles identified above:

a. **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.
b. **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.
c. **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.
d. **Designs detection measures** – Measures are implemented for detecting anomalies that could result from environmental threat events.
e. **Implements and maintains environmental protection mechanisms** – Environment protection mechanisms are implemented by Management to prevent and mitigate environmental events.
f. **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).
g. **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.
h. **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 an 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 that 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.

The type 1 report addresses the fairness of the presentation of management's description of the system and the suitability of the design of the controls at a point in time.

Management should evaluate the suggested complementary user controls and ensure that the controls the company has in place are adequate. Auditors will use this information in obtaining their understanding and testing of internal control. As noted earlier, management is responsible for the data that is entered into the company's financial reporting system no matter how it was processed. Management should also consider cybersecurity, data access, and vendor risk considerations associated with the service provider.

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.

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 complementary user control at the company was sufficient to mitigate the problem.

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.

III. Cybersecurity risks – Today's top cyber fraud schemes and how they work

Worldwide spending on cybersecurity has increased dramatically in the last several years and shows no sign of stopping. Recent cybersecurity research highlights the continued cost, persistence, and human element involved in cyber incidents[4]:

a. The average cost of a data breach was $4.88 million in 2024, the highest average on record (IBM);
b. 88 percent of cybersecurity breaches are caused by human error (Stanford);
c. The average time to identify a breach is 194 days (IBM);
d. The average life cycle of a breach is 292 days from identification to containment (IBM);
e. The likelihood that a cybercrime entity is detected and prosecuted in the U.S. is estimated at around 0.05 percent (World Economic Forum);
f. 68 percent of breaches involved a human element in 2024 (Verizon);
g. In 2023, security breaches saw a 72 percent increase from 2021, which held the previous all-time record (Forbes);
h. In 2022, the Federal Trade Commission received more than 1.1 million reports of identity theft (U.S. News);
i. Cyber fatigue, or apathy to proactively defending against cyberattacks, affects as much as 42 percent of companies (Cisco);
j. 64 percent of Americans have never checked to see if they were affected by a data breach (Varonis); and
k. The U.S. was the target of 46 percent of cyberattacks in 2020, more than double any other country (Microsoft).

The skill of threat actors has evolved alongside technological advancement, making it increasingly difficult for organizations to stay ahead of fraud risks. As new control mechanisms are implemented, threat actors adapt with more sophisticated attacks.

According to PwC's 2024 Global Economic Crime Survey, organizations today face a heightened risk of cyber-related fraud, particularly procurement fraud, which was reported as one of the top three most disruptive economic crimes across all industry sectors. Compounding the issue, many companies still underutilize data analytics in detecting fraud, leaving them vulnerable to threats that could otherwise be mitigated through proactive monitoring.

The survey emphasizes that technology is both a tool for good and a weapon in the hands of threat actors. Threat actors are now using AI to generate fake invoices, impersonate executives, and exploit business processes, blurring the line between cyber intrusion and traditional financial fraud.

It is important for companies and their auditors to understand the evolving fraud landscape and to strengthen not only technical cybersecurity defenses but also internal controls, vendor due diligence, employee awareness, and incident response protocols. Forward-thinking organizations are also investing in cyber fraud insurance and advanced transaction monitoring systems to reduce their exposure.

---

[4] https://www.varonis.com/blog/cybersecurity-statistics#data-breach-hacking.

There are several common types of cyber-attacks employed today. The attack types include phishing, whaling, social engineering, Distributed Denial of Service (DDoS) attacks, malware, and ransomware. And there are many variations of these attack types. Each of these categories continues to evolve as threat actors use automation, AI, and social engineering to increase the effectiveness of their attacks.

A. Authorized push payment fraud (APP)

APP fraud is a form of fraud in which victims are manipulated into making real-time payments to threat actors, typically by social engineering attacks involving impersonation. A threat actor commits this crime by convincing a business or person to send money for something that appears legitimate, like an invoice to what appears, to the victim, to be a recognized business. The invoices are convincing, with logos and the format that the impersonated business uses. The push part of the scheme comes when the victim authorizes a bank to make payment to an account that is not the impersonated business's account. Some threat actors will take over a victim's payment system and send money to payees without the victim's knowledge. It is only discovered when the victim looks at the bank account and notes the missing funds.

Push payments are very convenient ways to cut time off of transactions. They are prevalent in real estate transactions and are increasingly used in business-to-business payment environments.

Example: A threat actor is aware that a customer is about to purchase a home. Through phishing, social engineering, or impersonation techniques, 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 since been forwarded to a place where it generally cannot be reclaimed. Payment service providers (PSPs) have created software to detect unusual behavior and have even helped to try to reclaim money for victims.

APP fraud has become a significant issue in the United States, with sharp year-over-year increases in reported losses. According to ACI Worldwide, losses from APP scams in the U.S. are projected to rise to **$3.03 billion by 2027**, up from **$1.94 billion in 2022**, reflecting a growing threat across consumer and business payment channels.[5]

1. SMS spoofing

SMS (Short Message Service) spoofing is one tactic used to commit APP fraud. It uses technology to impersonate a trusted party such as a PSP as the sender of an SMS message. Victims receive messages that appear to be from their banks but are actually from threat actors and act out instructions believing them to be from their PSP.

B. Deep fakes and voice biometrics

Many companies and individuals use facial recognition to unlock cell phones or voice biometrics to command smart home devices. They seem like such a great security enhancement. However, threat actors use artificial intelligence to create fake images or audio manipulations to defraud companies. Victims who fall for this scheme can erroneously transfer cash to a threat actor's account. This type of spoofing is often paired with phishing emails or phone calls, and in some cases, deepfake voice messages have been used to impersonate executives or account managers. As generative AI tools

---

[5] ACI Worldwide. (2023). *Authorized Push Payment Fraud: An Escalating Threat.* Retrieved from https://www.paymentsdive.com/news/authorized-push-payment-fraud-banks-financial-services-ACI/702493.

become more sophisticated and accessible, the quality and realism of deepfakes continue to improve, making independent verification procedures increasingly important.

Example: "A finance worker at a multinational firm was tricked into paying out $25 million to threat actors 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)

C. Breaching multi-factor authentication (MFA)

Many companies and financial institutions use multi-factor authentication (MFA) controls such as SMS codes, authenticator apps, or biometric verification. However, threat actors continue to develop tactics to circumvent these defenses. One such method is SIM swapping, where attackers trick a mobile carrier into transferring the victim's phone number to a device under the attacker's control. This allows them to intercept MFA codes and complete account-takeover fraud. More recently, attackers have adopted a technique known as "MFA fatigue" or "push bombing," in which they bombard a user with repeated MFA approval requests until the user inadvertently accepts one. This tactic has been employed in several high-profile corporate breaches. Both SMS-based and app-based MFA methods are now being targeted, underscoring the need for risk-based authentication and ongoing user education.

Example: A threat actor visited a retail store of a mobile service provider. The threat actor 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 the threat actor's device, which she said was a spare phone. This enabled the threat actor to circumvent MFA since she would get the call instead of the real mobile customer.

D. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks overwhelm an organization's system resources, preventing it from responding to legitimate service requests. A key distinction is that DDoS attacks are launched from multiple compromised systems, often part of a botnet, whereas a traditional DoS originates from a single source.

These attacks do not usually involve unauthorized access. Instead, their purpose is to make systems unavailable. In some cases, threat actors may launch a DDoS attack as part of corporate sabotage or competitive disruption. More commonly, DDoS attacks serve as diversions to mask more serious intrusions such as data exfiltration, ransomware deployment, or credential harvesting.

For example, if the threat actor is working on behalf of a competitor, taking a company's system offline could significantly disrupt operations, providing a strategic benefit to the attacker and their employer. More often, however, denial of service techniques are used to disrupt systems in preparation for a more serious attack, such as ransomware deployment or data theft.

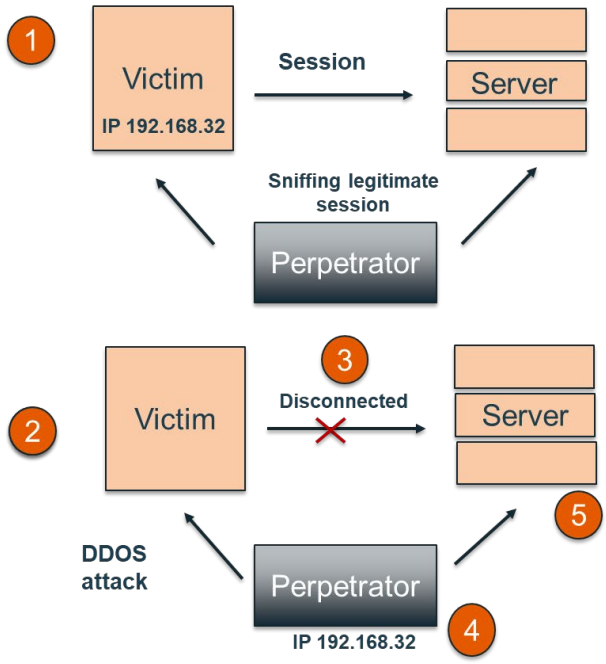
1. TCP SYN flood attack

One common type of DoS/DDoS exploit is the Transmission Control Protocol (TCP) SYN (synchronize) flood. In a standard TCP three-way handshake, a client sends a SYN packet to initiate a connection. The server replies with a SYN-ACK, and the client responds with an ACK to complete the handshake.

In a SYN flood, the attacker sends a large number of SYN requests without responding to the server's SYN-ACK replies. This fills the server's connection queue and ties up system resources waiting for

responses that never come. When the queue overflows, the system may crash or become temporarily unresponsive.

As illustrated in the diagram, the attacker spoofs the client's IP address, interrupts the session, and tricks the server into thinking it is still communicating with a legitimate client, when in reality, the server is under a denial-of-service condition.



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.

There are a few possible solutions to prevent a TCP SYN flood attack:

a. Place servers behind a firewall configured to stop inbound SYN packets.
b. Increase the size of the connection queue and decrease the timeout on open connections.

2. Teardrop attack

This legacy attack exploits a vulnerability in older operating systems' handling of fragmented Internet Protocol (IP) packets. It manipulates the length and fragmentation offset fields so that packet segments overlap when being reassembled. When the target system attempts to reconstruct the corrupted packet sequence, the process fails, often resulting in system instability or a crash.

Note:

Most modern systems have patched this vulnerability, but it's a useful example of how protocol-layer exploits can lead to denial-of-service conditions.

3. Smurf attack

This attack uses Internet Control Message Protocol (ICMP) and IP address spoofing to overwhelm a network with traffic. A threat actor spoofs the IP address of a known, trusted system and sends ICMP echo requests (pings) to the broadcast address of a network. When multiple devices on the network respond to the spoofed request, the flood of responses saturates the target system. This attack relies on

misconfigured network devices that respond to broadcast ICMP requests. Today, most modern networks and routers are configured to block this behavior by default.

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 overwhelm the network.

Solution: Configure routers and network devices to block directed broadcasts and restrict responses to broadcast ICMP requests.

4. Ping of death attack

In a ping of death attack, a threat actor sends Internet Control Message Protocol (ICMP) echo requests (pings) that are larger than the maximum allowable IP packet size. To bypass this limit, the oversized packet is broken into smaller fragments. When the target system attempts to reassemble the fragments, it may experience buffer overflows, crashes, or system instability. Most modern operating systems are no longer vulnerable to this attack, but firewalls should still be configured to check fragmented packets for abnormal sizes as a preventative measure.

5. Botnets

A botnet is a network of internet-connected devices, such as computers, routers, or IoT devices, that have been infected with malware and are controlled remotely by a threat actor. Each infected device is called a bot. Botnets are commonly used to send spam, harvest credentials, deploy ransomware, or launch distributed denial-of-service (DDoS) attacks. In DDoS scenarios, thousands (or millions) of bots are directed to flood a target with traffic, overwhelming its bandwidth and computing resources. Mitigation strategies include implementing source address validation techniques such as RFC 3704 filtering and using “black hole filtering” to drop malicious traffic before it reaches critical systems.

6. Ransomware and ransom attacks

Ransomware is malware that infects IT systems, halting user activity until a ransom is paid. Ransomware is not new, and at one time threat actors required payment through the US mail. As technology has evolved, payment is now generally demanded by Bitcoin or other digital payment methods. Law enforcement officials recommend that a victim refuse to pay the ransom. The malware often enters the system through phishing email.

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.

Ransomware attacks would be difficult to accomplish without cryptocurrencies (e.g., crypto assets) that allow anonymous payments and receipts outside of traditional bank reporting requirements.

Solution: Back up the system hourly on an unrelated server.

E. Phishing and spear phishing attacks

Phishing occurs when a threat actor sends emails that appear to come from trusted sources in order to steal sensitive information or manipulate the recipient into taking harmful action. These attacks combine social engineering and technical deception. Phishing messages may contain attachments that install malware or links to spoofed websites designed to harvest credentials or install malicious software. Spear phishing is a targeted form of phishing in which the attacker researches the victim's habits, contacts, or language patterns to craft a message that appears credible and highly personalized. These emails often include email spoofing, where the "From" field appears to come from someone the victim knows, usually someone with authority, such as a supervisor or executive. Another technique is website cloning, in which a legitimate website is duplicated and used to collect login credentials or personally identifiable information (PII). In recent years, phishing has become more sophisticated through the use of generative AI to write more convincing emails, and it is frequently associated with business email compromise (BEC) attacks and may include QR-code phishing ("quishing") that directs users to malicious websites.

While technology can help filter out many phishing emails, human awareness and manual intervention remain essential. Organizations should train employees to:

a. **Stop and think** – Don't assume the sender is legitimate simply because the name looks familiar. Threat actors rely on impulse responses.
b. **Hover over email addresses and hyperlinks** – Inspect the actual URL before clicking. A mismatch between the visible link and the actual destination is a red flag.
c. **Review email headers** – Check that the "Reply-To" and "Return-Path" parameters match the domain of the sender. Discrepancies may indicate spoofing.
d. Use extra caution with QR codes, especially when they appear in emails, invoices, or unexpected messages.

F. Drive-by download attacks

Drive-by download attacks are a common method of spreading malware. The threat actor looks for an insecure website and places a malicious script into the code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might redirect 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.

Unfortunately, a drive-by attack doesn't always rely on a user to do anything to actively enable the attack. Since the victim doesn't have to click anything or open an email attachment to get infected it is harder to prevent. A drive-by download can take advantage of an app, operating system, or web browser that contains security flaws due to unsuccessful updates or lack of updates.

To reduce risk, users should keep browsers and operating systems fully updated and avoid visiting untrusted websites. The more browser extensions or plug-ins a device has installed, the larger the attack surface becomes.

G. Password attacks

Passwords are the most commonly used mechanism to authenticate users to an information system. Therefore, a threat actor may try to attack by guessing passwords. Threat actors will sometimes look around at 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. Password attacks are also frequently combined with phishing, MFA fatigue, or credential theft from prior breaches.

A threat actor has several methods they can use:

a. **Brute-force** or targeted password guessing – Brute-force attacks use automated tools to try large numbers of possible passwords, while targeted password guessing uses information known about the user, such as their name, job title, hobbies, children, or pets, to improve the likelihood of success.
b. **Dictionary attack** – The threat actor copies an encrypted file that contains the passwords; they apply the same encryption to a dictionary of commonly used passwords and compare the results.
c. **Credential stuffing** – Using stolen usernames and passwords from one breach to gain access to other accounts, exploiting password reuse across platforms.
d. **Password spraying** – Attempting a few commonly used passwords (e.g., "Welcome123") across many accounts to avoid account lockouts.

H. Cross-site scripting attacks

Cross-site scripting (XSS) attacks occur when a threat actor exploits a vulnerability in a legitimate website to execute malicious scripts in a visitor's web browser. These scripts are typically written in JavaScript and are executed without the user's knowledge when they load or interact with the compromised page.

The attacker injects malicious code, often via user input fields or URL parameters, into a web page that fails to properly validate and sanitize the input. When a victim visits the site, the script is executed in their browser as if it were part of the trusted website.

At minimum, the attacker may hijack a session or deface content. At worst, XSS can allow the attacker to steal session cookies, log keystrokes, capture screenshots, collect system or network data, or even remotely control the victim's device.

To prevent XSS, developers should implement input validation and output encoding (escaping) to ensure all user-supplied data is properly sanitized before being rendered in the browser. They should also avoid reflecting raw input data in responses without filtering or encoding it. In addition, developers can strengthen protection by implementing Content Security Policy (CSP) headers and, where feasible, offering users the option to disable client-side scripts.

I. Eavesdropping

In an eavesdropping attack, a threat actor intercepts network communications to capture sensitive information, such as login credentials, credit card numbers, or proprietary data. These attacks can occur on unsecured or poorly configured networks, particularly public Wi-Fi.

Passive eavesdropping involves quietly monitoring unencrypted transmissions without directly interacting with the communication. In contrast, active eavesdropping may involve man-in-the-middle (MITM) techniques, in which the attacker impersonates a trusted device to intercept, modify, or inject traffic between two parties.

To defend against eavesdropping, organizations and individuals should use strong encryption protocols, such as TLS (Transport Layer Security), VPNs (Virtual Private Networks), and HTTPS, and secure Wi-Fi configurations, for all network communications. Sensitive transactions should not be conducted over unsecured public networks unless encryption is properly enforced.

J. Malware

Malicious software (malware) is installed on a victim's system by a threat actor. It can attach itself to legitimate code, spread across devices, or remain hidden within useful applications. Malware can replicate itself across networks or be deployed through phishing, infected downloads, malicious links, or compromised websites. There are many types of malware, some of which are described below:

a. **Macro viruses** infiltrate programs most people use every day such as Microsoft Word or Excel. These 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.

b. **File infectors** attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded.

c. **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.

d. **Stealth viruses** compromise malware detection software so that the software will report an infected area as being uninfected.

e. **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.

f. **Worms** do not attach to a host file. They are self-contained programs that spread across networks and computers, usually through email attachments. The victim opens an attachment and activates the worm program. The worm then sends a copy of itself to every contact in the victim's email program. This enables it to spread across the internet, conduct malicious activity and overload email servers which can result in DoS attacks.

g. **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. In recent years, ransomware has evolved into a "ransomware-as-a-service (RaaS)" model, where threat actors sell or lease the malware to affiliates who carry out the attacks. Many ransomware attacks now also involve data theft and extortion, where threat actors threaten to release sensitive information even if systems are restored from backup.

K. Internet of Things (IoT)

The Internet of Things (IoT) extends internet connectivity beyond the normal devices we all use such as computers, tablets, smart phones, etc. and makes it possible for household devices and other objects to interact over the internet. A familiar example is a voice-activated virtual assistant, but IoT also includes everything from smart appliances to industrial sensors. IoT devices can be categorized into three primary groups.

Group	Application
Consumer	Smart security, smart speakers, smart air conditioning, pacemakers, 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 automatically during presentations.
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.

These are very helpful applications. However, as the number of connected devices grows, so does the potential attack surface. Current IoT risks affect consumer, enterprise, and industrial environments and include weak default passwords, unpatched firmware, insecure device configurations, poor device discovery, unauthorized access, and botnet-driven attacks such as DDoS. Organizations should inventory connected devices, change default credentials, apply updates, segment networks, and monitor IoT activity as part of their cybersecurity program.

L. It's also a people problem

Threat actors are creative and become more so every year. Entities should have the best protection they can afford and there are a number of technological solutions available. However, without getting a handle on the entity's "people problem," technology may be thwarted or diminished. Threat actors use social engineering to gain a foothold in an entity's information technology system. Combating social engineering takes training, focus, and reinforcement.

Social engineering involves manipulating people so they will divulge confidential information that the threat actor can use to gain access into the system. According to Verizon's 2024 Data Breach Investigations Report[6], the human element was a factor in 68 percent of data breaches, and social engineering tactics, including phishing and pretexting, accounted for 73 percent of incidents within that attack category. These tactics are commonly used to obtain login credentials and financial information or to deploy malware that enables broader access. Educated and security-conscious employees remain the strongest defense against social engineering attacks. In cybersecurity, trust must be earned. Users should always ask: *"How do I know this communication is legitimate?"*

Once threat actors obtain a single password, they can access contact lists and use the compromised account to launch further attacks. These attacks may include sending malicious links, impersonating the original victim, or embedding malware in seemingly innocuous downloads. Even hovering over email addresses to verify authenticity can be bypassed with advanced spoofing. Threat actors frequently impersonate companies by sending emails that appear legitimate, complete with logos and language commonly used by banks. Financial institutions remain common targets for impersonation in phishing campaigns. Threat actors use a variety of tactics, such as asking for donations, presenting false problems that require "validation" of personal info, offering free gifts, or pretending to be coworkers or executives. AI-enabled tools can make these messages more convincing by imitating tone, writing style, voice, or video. These attacks affect both personal and corporate email accounts.

[6] Verizon. 2024. *Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/.

Solutions:

a. Slow down. Nothing is that urgent that it should not be carefully reviewed.
b. Call to confirm. Oral verification, despite being time consuming, is worth it, especially for payment changes, wire transfers, or urgent executive requests.
c. Visit the organization's official website in a new browser window rather than clicking embedded links.
d. Delete any requests for financial information or passwords.
e. Be suspicious of offers to help (e.g., restore credit scores, refinance a home, etc.).
f. Secure computing devices with anti-virus software, firewalls, email filters and update them regularly.
g. Train employees regularly and enforce penalties for violating cybersecurity protocols.

Example 1: 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.

Example 2: 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.

M. Statistics that are good to know

Varonis published the following statistics related to the part employees may inadvertently play in cybercrime:

a. 91 percent of malware was delivered by email (Deloitte).
b. 19 percent of 2022 data breaches were caused by stolen or compromised credentials (IBM 2022).
c. 45 percent of data breaches occurred in the cloud (IBM 2022).
d. 83 percent of organizations had more than one data breach, at an average cost of $4.35 million per breach (IBM 2022).

According to Varonis, worldwide cybercrime costs are estimated to hit $10.5 trillion annually by 2025 (Cybersecurity Ventures), and global spending on cybersecurity products and services is predicted to reach $1.75 trillion cumulatively for the five-year period from 2021 to 2025 (Cybersecurity Ventures).

Example: Tech Beacon's dangerous app survey identified the following high-risk iOS apps that have been banned by employers on company-provided mobile devices:

a. WhatsApp Messenger;
b. Pokémon GO;
c. WinZip Utilities;
d. CamScanner Productivity;
e. Plex;
f. WeChat;
g. Facebook Messenger;
h. eBay Kleinanzeigen;
i. NetEase News; and
j. Device Alive.

The biggest issues identified were sending SMS messages or sensitive data without encryption, accessing address books and cameras without permission, and tracking a phone user's location.

IV. Internal control imperative

Companies are accustomed to designing a system of internal control primarily to prevent, detect and correct fraudulent financial reporting and misappropriation of assets from internal sources or internal sources colluding with outsiders. General computer and application controls are designed for this purpose. However, with the scrutiny on cyber fraud today, it may be time to increase the level of cyber fraud assessment and address control weaknesses.

A. SEC cyber fraud report

The SEC has investigated numerous cases in which companies experienced significant financial losses due to cyber-enabled fraud schemes, resulting in nearly $100 million in losses across nine companies. The techniques used by the threat actors are common. Company personnel received spoofed or compromised electronic communications from outsider sources causing them to transfer funds to the bank accounts of the threat actors.

One of the companies cited in the report made 14 electronic transfers based on fictitious emails received from threat actors 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 threat actor's bank account. Today, similar schemes are often associated with business email compromise (BEC), vendor impersonation, and AI-enhanced social engineering attacks.

The SEC did not institute enforcement actions against the companies but made it clear in the report that public companies subject to Section 13(b)(2)(B) of the Securities Exchange Act, which is the federal law covering internal controls, will be required to assess and adjust their internal controls for the risk of cyber fraud. This guidance remains relevant today as cyber fraud continues to pose material risks to financial reporting.

Section 13(b)(2)(B) of the Securities Exchange Act is invoked when a public company has:

a. Materially misstated its financial statements;
b. Paid bribes to foreign government officials;
c. Paid commercial bribes; or
d. Reimbursed employees for unauthorized expenses.

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. The 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. They are used by the SEC in connection with bribery and expense reimbursement prosecutions where the financial ramifications are generally not material for financial statement purposes.

The cases discussed in the report did not involve sophisticated schemes. Human weakness made them effective. The COSO framework is specific in saying that controls only provide reasonable, not absolute assurance.

The 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. This includes nonpublic entities as well, even if it is because cyber fraud is costly to an entity's financial position and reputation.

B. Internal controls to help prevent cyber fraud

Entities should consider:

a. A robust cyber fraud risk assessment process;
b. Establishing more stringent cybersecurity policies and procedures;
c. Performing scenario analysis, including how management could override controls;
d. 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;
e. Identifying key controls over changes to vendor disbursement processes;
f. Evaluating the design and periodically testing controls;
g. Obtaining a cyber fraud diagnostic from a qualified third-party provider;
h. Training personnel and penalizing those who violate the controls even through carelessness;
i. Monitoring activities with data analytic tools for potential improper disbursements; and
j. Requiring independent verification for vendor banking changes, urgent payment requests, and other high-risk disbursements.

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 remote location. Applications and infrastructure are placed behind the organization's firewall and therefore are 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. Preventive 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 preventive controls fail to detect and mitigate the threat before a user sees it, endpoint protection may add an additional mitigation step to prevent unauthorized use of computer resources.

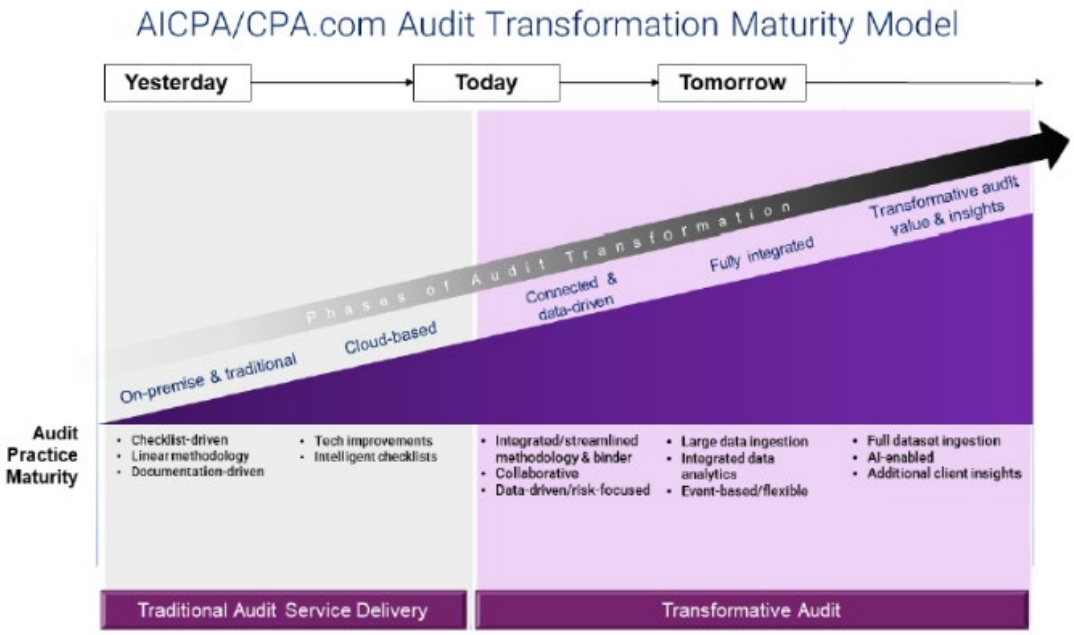
Public company management should also consider disclosure controls for cyber breaches due to section 302 certifications and applicable cybersecurity disclosure requirements.

Discussion question:

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

1. New section: Audit transformation

Traditionally, audits were primarily conducted through document-checklist methods. However, the adoption of cloud computing, AI, and data analytics has transformed this approach, enabling audits to be performed more efficiently and effectively. Auditors are currently advancing to the next phase of audit transformation, as depicted in the "AICPA/CPA.com Audit Transformation Maturity Model" graphic shown below. As the field progresses, further enhancements and deeper insights into engagements are expected. This will be driven by auditors adopting fully integrated, knowledge-driven methodologies that leverage AI and other technologies.



For several years, the AICPA has advocated for the integration of technology to revolutionize the audit process. In line with this initiative, the AICPA has collaborated with CPA.com, numerous prominent accounting firms, and technology partner Caseware International to create the Dynamic Audit Solution (DAS). This initiative combines a data-driven methodology, guided workflow tools, and data analytics within a unified 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.

A recent practice aid from the ASB's Technology Task Force titled "Use of Technology in an Audit of Financial Statements" aids auditors in refining their risk assessments. This document explains and demonstrates through examples how technology can enhance both the effectiveness and efficiency of audits. It initially concentrates on the process of risk identification and assessment as outlined in Statement on Auditing Standards (SAS) No. 145.

As firms increasingly incorporate AI-assisted tools into audit workflows, auditors remain responsible for exercising professional skepticism and evaluating whether technology-generated outputs provide sufficient appropriate audit evidence.

C. 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:

a. To understand the nature, timing, and extent of the audit procedures performed to comply with professional and legal requirements; and

b. To understand the results of the audit procedures performed and the audit evidence obtained.

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:

a. The identifying characteristics of the specific items or matters tested;
b. Who performed the audit work and the date such work was completed; and
c. 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. 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.