Technology Trends and Hot Topics Impacting the Accounting Profession

THT4/23/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 with 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
- On-Site 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.

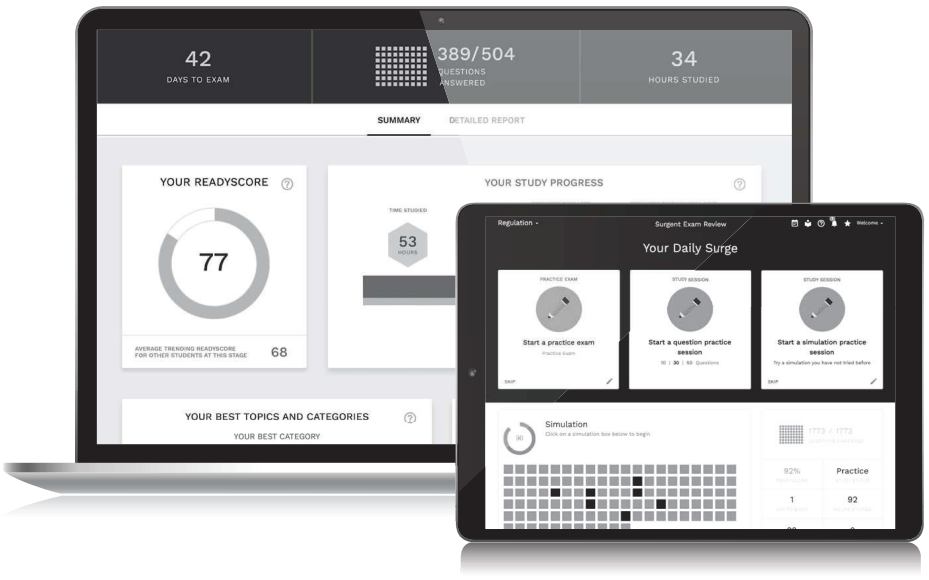
(484) 588.4197
salesinfo@surgent.com

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

Revised June 2023

Data-Driven Decision Making

Data-Driven Decision Making

Learning objectives

Upon completing this chapter, the reader will be able to:
- Identify the standards that are on the horizon to be issued in the next two years; and
- Understand the significant changes that are likely to occur.

I. Introduction

Companies are under an immense amount of pressure today. The business environment continues to be more and more 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 from competitors they never expected. For example, not only has Amazon disrupted sales in retail stores, in 2017 it entered the grocery market through its acquisition of publicly traded Whole Foods Market.

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. The main driver of this trend is advances in technology. In fact, digital is the reason that over half the Fortune 500 companies have gone under since 2000. Consider the fate of Blockbuster, a company that was unable to change with the times and compete with companies like Netflix. And some companies, such as Kodak, came out of bankruptcy and switched gears. Kodak is now a technology company focused on imaging, hardware, software, and consumables to customers in 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 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.

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% more on Amazon.

A. Disruption in the accounting profession

Finance and accounting professionals need to consider embracing continuous learning that goes past traditional continuing professional education. New competencies will be needed to succeed in a digital world. In 2016 a Bank of America Report estimated a 90 percent or more risk of accountants being

replaced by robots. This reinforced a 2013 Oxford University study that finds 94 percent of accountants and auditors were at risk of job loss due to automation. While it is true that certain accounting tasks are already being performed by robots, the accounting and finance professions are by no means on their way out. In fact, finance and accounting professionals can play a large role in data-driven decision making and the functions are likely to be judged on how much value they add to the entity. The time freed up by automated processing combined with new technologies will create time for value added tasks.

The changes that seemed looming in 2013 and 2016 did not materialize as quickly as anticipated but it is easy to see that technological advances are being embraced by companies, especially larger ones and they are expecting their auditors to be up to the challenge. In “2020’s Vision: Tech Transformation on Tap,” an article published in the Journal of Accountancy online in January 2020, it is clear that the past 10 years or so have been about streamlining the processing of expenses and bills in putting information into the general ledger through automation and the reading of documents by optical character recognition (OCR). Advances have already led to machine learning and more sophisticated predictive analytics which aids in interpretation of data.

Accounting firms will very likely look for more people with a digital mindset and knowledge of technology who will be able to set up the inquiries and tests as well as interpret the results from advanced analytics and other technologies. There is some concern that clients may expect a drop in fees if audits become more automated, not seeing that the costs to invest and perform audits is not likely to decrease. Later in this course we will discuss the opportunities and risks that advanced data analytics and other technologies bring.

The AICPA and NASBA are working to evolve the initial CPA licensure requirements. The modifications in requirements validate some of the changes that colleges and universities are already making to the accounting curriculum, integrating technology skills that are now and will become even more necessary for the accounting profession.

B. Drivers of change in a digital world

The 2019 CGMA (Chartered Global Management Accountant) whitepaper, *Reinventing Finance for a Digital World*, discusses four main drivers of a digital world. Technology is not the sole driver of change. There are many other forces at play as well.

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 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** (distribution of world power) and **regulation** have a very significant impact on the supply chain. The balance of power continues to move south and east in the world. Countries are investing in AI and data to compete internationally.
Social	There are presently **6 generations** living in the same space. More than half of the people live in urban areas. This makes it more challenging for companies to focus and doubly important to understand the patterns of behavior in the way people use technology and the way they consume.

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 organizations. 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 there. It lies in the 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. Depending on the egos involved, this is where a data-driven organization quickly breaks 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, 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. Barriers to data-driven decision making

1. HIPPO effect

Dylan Lewis from Intuit introduced the acronym HiPPO at a conference in 2006. He was discussing the power of using consumer research rather than the highest person's opinion. Next, the term was modified to HiPPO (highest paid person's opinion) by Avinash Kaushik in his book, *Web Analytics: An Hour a Day*. People tend to trust the person with the most power and experience and even when some don't, they tend to go along with that person because they do not want to make a dissent even when they know a mistake is being made. Even back as far as 1963 with the Milgram Experiment, researchers have known that there is a conflict between obedience to an authority figure as opposed to following one's own conscience. This stems from the tendency to believe the "experts" and authority figures. Subsequent experiments bear this out. In 2016 the Rotterdam School of Management performed a study that demonstrated that projects led by senior leaders failed more often while projects led by junior managers were more likely to be successful. This phenomenon is believed to be due to the junior managers having the benefit of critiques to their projects that helped make them stronger where employees did not feel comfortable providing feedback to senior leaders. In 2012 the COSO (Committee of Sponsoring Organizations) commissioned a study published as *Enhancing Board Oversight: Avoiding Judgment Traps and Biases*. The COSO report discusses the elements that are detrimental to boards in making sound judgments. Chief among them were the tendency to blindly accept the opinions of the highest-ranking members or perceived experts without asking questions.

2. Other barriers to 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.

In 2016 SAS sponsored a research project which was published by Harvard Business Review called the *Evolution of Decision Making, How Leading Organizations Adopt a Data-Driven Culture*. The article 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 with 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 what data went into the data analysis process and the algorithms used to analyze the data. The decision maker needs to be data literate 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. More than half of the people in high level positions are not data literate. 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.
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.

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 is appropriate for the decision to be made. It is important that data is clean and reliable 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 for making the decision needs to be relevant to the problem that the analyst is trying to solve.
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.
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?

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:

- Provide robust data ingestion, integration, and preparation features;
- Consume data through file uploads, data base querying, and application connection;
- Create reports and visualizations with business utility; and
- Create and deploy internal analytics applications.

G2, a clearinghouse of information related to reviews of BI software, performed an analysis of the reviews received through mid-2020. Following is a table that presents the highest performing data analytic products.

Product	Reviewer Satisfaction Score (1-100)	G2 Score (1-100)
Domo	91	94
Looker	94	92
Tableau	88	92
Sisense	94	91
Insight Squared	96	83
Mode	75	82
Board	90	81
Chartio	63	78
Klipfolio	89	78

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. 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.

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 authentication. 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.

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

- In transit from a computer to a storage device or over a network.
- Hardware failures in storage devices or the computer itself can occur.
- Software or security applications can be misconfigured resulting in damaged data.
- A deliberate breach can occur where a person or software hacks into a system and changes data. For example, malware (ransomware) encrypts data and holds it hostage for payment. Alternatively, a hacker may breach the system and make changes.

Data integrity has several important aspects:

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

The system should have:

- Controls to validate the input;
- Controls to validate the data itself;
- Controls to create backups;
- Access controls; and
- 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, and enforcing new policies and procedures.

Technology Trends and Risks

Technology Trends and Risks

Learning objectives

Upon reviewing this chapter, the reader will be able to:
- Identify and discuss the top 10 technology trends and risks;
- 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 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 ChatGPT.
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. Mobile Accountants.
10. Changes in Professional Literature and Internal Control Guidance.

A. Cloud computing

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

- Transactional data;
- Data collected from the IoT (internet of things) which could be data from appliances, consumer wearables, temperature checking devices, devices such as Alexa that track activities by the user and more; and
- Data on customers collected from questions asked by point of service devices.

Many IT systems are not equipped to handle the volume of data.

Cloud computing is essentially outsourcing the processing of an entity's data to a network of remote servers hosted on the internet. Since cloud computing is scalable, both small and large entities can use it. Companies would no longer need to buy and maintain IT expensive systems. In addition, the robust processing power is a significant benefit. This is very important when it comes to performing advanced data analytics and using AI.

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.

Example:	A programmer was developing an RPA application. It was written to: • Download a file; • Take certain data from the file; • Transfer that data to another file; and • Save the document. This set of repetitive tasks, which was previously performed by an employee, did not involve decision making. The RPA application saved the company 400 person hours a year and accuracy improved.

C. Artificial intelligence

The use of artificial intelligence (AI) is growing in prevalence and in scope. AI can read contracts, write memos, summarize documents, perform automated tasks, and identify risks. 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. Like any new technology, the users will go through a phase of wondering if the output can be trusted. In addition, if AI provides the user with an answer, they may want to understand how the program came to that determination. Although this may be wanted, it is not always possible with certain algorithms, like large language models (LLMs), that do not follow an auditable decision structure.

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 an anomaly or not.

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

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

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

This type of machine learning is extended for LLMs. Large language models have the ability to generate text, tables, and responses by "learning" on large quantities of data to identify patterns and trends. For example, ChatGPT, the most well-known LLM operated by open.AI, was trained on over 8 million web pages before its launch. This large amount of training data allows the LLM to make billions of connections for every prompt and response, making it difficult to understand how or why a given response was created by the LLM when prompted.

LLMs are designed to provide human-like responses. They can be asked to write in a particular style, format, or for a specific audience. The quality of their answers improves as users refine their prompts and engage with the LLM.

D. Advanced data analytics

Companies and auditors already use data analytics. With the explosion of data coming from the IoT, social media and mobile computing, 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% without approval. The auditor went back and performed a further analysis to determine if the percentage discounts on sales of product increased and determined that this was the anomaly in sales. This insight was added to the substantive analytical procedure. In addition, the auditor was able to let the sales manager and the CFO understand the ramifications of the policy change.

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 from the past several years. She observed that outside temperatures were correlated with sales. Other factors that appeared to play a role were school holidays. She used this data as well as the predicted weather forecast for the upcoming period to estimate demand.

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.

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.

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.

F. Outsourcing the accounting function

Some businesses are outsourcing their entire accounting functions to third parties so they can concentrate on operations. IBISWorld noted that between 2017 and 2022, the global BPO industry grew at a compound annual growth rate of 2.2%. BPO providers have economies of scale and typically operate in low-cost countries. By outsourcing the accounting function an entity does not have to invest in the technology that continues to improve each year. Outsourcing has its drawbacks. Data breaches, quality issues and perhaps being in a country with an unstable government can have a big impact on a company. Quality and the level of internal controls over financial reporting and compliance should be a prime concern when considering outsourcing the accounting function.

G. Accounting and finance professional will need different skill sets

The biggest challenge that companies accounting firms will face going forward is that employees that have been out of school for more than a couple of years do not have the right skill sets. A survey by Robert Half asked approximately 1,100 CFOs about their needs and challenges finding qualified personnel.

37% of CFOs said that business analytic skills were mandatory for everyone. 49% said that they were mandatory for certain positions. 12% said they were nice to have but not mandatory. 2% 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 aptitude and help them improve in the areas needed.

As a client's IT system becomes more integrated and the technologies the client is employing become more sophisticated the composition of the audit team may need to change. When choosing audit team members to understand and test IT controls, it is also important that they understand the system development lifecycle for emerging technologies. Traditional audit team members may not have deep expertise in IT. 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 a person with specialized skills is 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[1] 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.

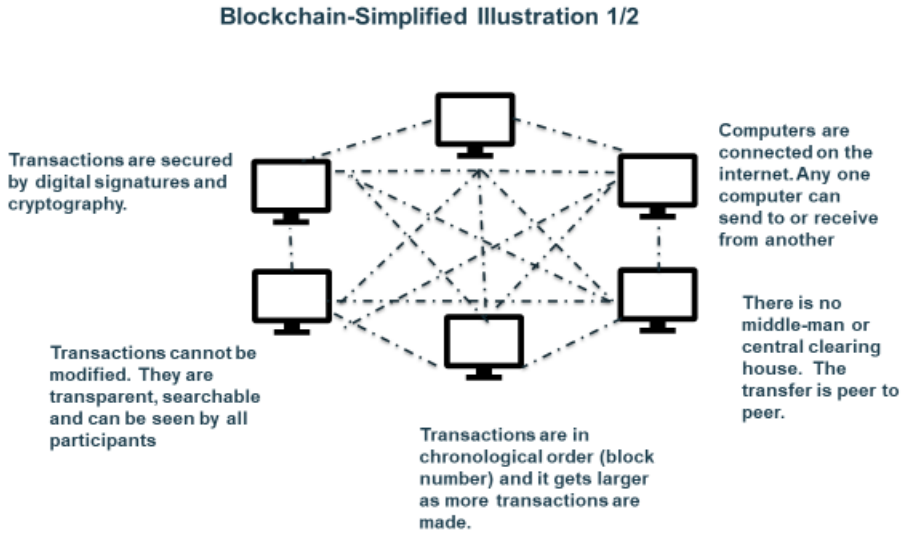
The "block" is a record of a new transaction and when it has been verified it is added to the chain. If an individual or company owns bitcoin they have a key (password) to an address on the chain and that is where their ownership is recorded. There is no centralized processing entity (middleman) needed 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,

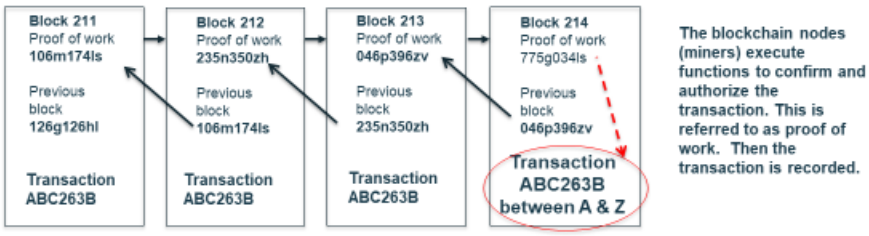
---

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

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*.[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.

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.

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

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 hackers 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. Mobile accountants

With the emergence of cloud computing and acceptability of electronic documentation as opposed to evidence that is in paper form, accountants are more able to work remotely. Although some firms performed primarily remote audits, this appears to be an emerging trend.

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. Chapter 3 will focus on the changes to the AICPA's Evidence Standard that became effective on December 15, 2022. 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:
   - The entity identifies risks to achieving its objectives and analyzes risks to determine how the risks should be managed; and
   - 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

- 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.
- 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.

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

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:

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

The auditor will also want to talk with those charged with governance to see how the board, or audit committee, is overseeing the impact of emerging technologies on financial reporting. If the entity has an internal audit department it is important to understand their role, if any, in IT auditing.

Auditors will want to understand:

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

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:

- Complete, accurate, valid data; and
- 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:

- **Input controls** – These controls are designed to ensure that the data entered into the system is complete and accurate.
- **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.
- **Output controls** – These controls are designed to ensure that reports produced by the system are distributed to only authorized personnel.
- **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 comprehension 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:

- Access;
- Change and incident management;
- Systems development;
- Data backup and recovery; and
- 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:

- Vendors can access the system only for a short period after installation;
- Terminated employees no longer have access to the system; and

- When job responsibilities are changed, access to data is also changed.

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

   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:
   - System updates were properly installed; and
   - 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 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 than 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:

- Procedures used to initiate, authorize, record, process and report information in the financial statements whether automated or manual;
- Related accounting records, whether electronic or manual, supporting information and specific accounts in the financial statements;
- How the information system captures events and conditions, other than classes of transactions that are routinely processed;
- Process used to prepare the entity's financial statements including significant accounting estimates and disclosures;
- Procedures and technology such as firewalls used to safeguard the entity's data; and
- Extent of cybersecurity 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 error such as incomplete, inaccurate or invalid record transfers between systems. If the software detects a possible error it attempts to resend the record. If the error persists the system sends an email to an operator so they can correct the error. Financial management is notified of errors in a weekly report. This way adjustments can be made to the system if necessary. The controller reviews and approves changes to the systems.

2. Unauthorized access to data

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, and required parameters such as password format and a requirement to periodically change passwords.

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:

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

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

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

There are three principles related to data availability:

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

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

- **Current Usage** – Measurement of use of system components is performed to establish a baseline for capacity management and to refer to when evaluating the risk of lack of availability due to capacity constraints.
- **Forecasts Capacity** – A forecast and comparison of expected average and high use of system components to system capacity and tolerances is performed. Considerations include capacity in the event there is a system failure.
- **Identifies Environmental Threats** – Management identifies environmental threats as part of the risk assessment that could impair the availability of the system. These could include threats resulting from weather, failure of environmental control systems, electrical discharge, fire, and flood/water.
- **Designs Detection Measures** – Measures are implemented for detecting anomalies that could result from environmental threat events.
- **Implements and Maintains Environmental Protection Mechanisms** – Environment protection mechanisms are implemented by Management to prevent and mitigate environmental events.

- **Responds to Environmental Threat Events** – Procedures have been developed and put in place for responding to environmental threats and for evaluating the effectiveness of those policies and procedures on an ongoing or periodic basis. This includes, but is not limited to, automatic mitigation systems (i.e., UPS and generator back-up subsystem).
- **Implements Business Continuity Plan Testing** – Business continuity plan testing is performed on at least an annual basis. The testing includes: (1) developing testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from the entire entity that can impact availability; (3) scenarios that consider the potential for lack of availability of key personnel; and (4) updating continuity plans and systems based on test results.
- **Tests Integrity and Completeness of Back-Up Data** – The integrity and completeness of back-up information is tested on at least an annual basis.

8. Risks introduced when using third party service providers

Various risks can be introduced when the company uses an outsourced service provider. Management should obtain 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, the suitability of the design of the controls at a point in time.

Management should also evaluate the suggested complimentary user controls and ensure that the controls that 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.

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 complimentary 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. According to a report from Varonis (110 Must-Know Cybersecurity Statistics for 2020)[3]:

- 62% of businesses experienced phishing and social engineering attacks in 2018.
- 68% of business leaders feel their cybersecurity risks are increasing.
- Data breaches exposed 4.1 billion records in the first half of 2019.
- 71% of breaches were financially motivated and 25% were motivated by espionage.
- 52% of breaches featured hacking, 28% involved malware, and 32–33% included phishing or social engineering.
- Between January 1, 2005 and April 18, 2018 there were 8,854 recorded breaches.
- The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%.
- Hackers attack every 39 seconds, on average 2,244 times a day.
- The average time to identify a breach in 2019 was 206 days.
- The average cost of data breach is $3.92 million as of 2019.
- 51% of businesses experienced denial of service attacks in 2018.

In addition:

- Gartner reported that worldwide spending on cybersecurity is forecasted to grow 11.3 percent in 2023.
- CNBC reported that phishing attacks were up 61% in 2022 over 2021
- Data breaches exposed 1.2 billion records in 2022 in the top 35 breaches alone according to Forrester research

The skill of cyber criminals has evolved along with the rate of change in technology. When security experts devise solutions to one scheme, another more sophisticated scheme appears. Cybercrime was identified in PWC's Global Economic Crime and Fraud Survey (2018) as the most disruptive type of fraud. The types of cyber fraud that affected entities according to that study follow.

Disruption of business processes	30%
Extortion	21%
Asset Misappropriation	24%
Intellectual property (IP) theft	12%
Procurement fraud	11%
Insider trading	10%
Politically motivated or state sponsored attack	5%

The study differentiates between digital **theft** and digital **fraud.** Digital theft schemes include stealing cash, personal information, and intellectual property. Digital fraud is longer lasting and more disruptive because the fraudster penetrates an open door which is usually a customer- or employee-facing access point and uses the company's own business processes to attack it.

[3] https://www.varonis.com/blog/cybersecurity-statistics/.

It is crucial for companies and their auditors to understand the general landscape of metrics surrounding cybersecurity issues, including what the most common types of attacks are and where they come from. Companies should also take steps to educate their employees and implement control mechanisms including manual controls to prevent attacks. Cyber fraud insurance can also help.

There are several common types of cyber-attacks employed today and there are many variations on those attack types. The attack types include phishing, whaling, social engineering, Distributed Denial of Service (DDoS) attacks, malware, and ransomware. And there are many variations on these attack types.

A. Authorized push payment fraud (APP)

APP fraud is a form of fraud in which victims are manipulated into making real-time payments to fraudsters, typically by social engineering attacks involving impersonation. A fraudster 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 fraudsters 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.

Example:	A fraudster is aware that a customer is about to purchase a home. Through phishing or social engineering, they cause the customer to create an authorized push payment but instead of the money ending up in an escrow account or the seller's account it goes to a fraudulent account. Because it was authorized, the bank has no responsibility. By the time it is evident that this has occurred the money has long 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.

This is a very prevalent scheme in the United Kingdom, which is now being seen in the United States. In the first six months of 2019, fraudsters stole 207 GBP from unsuspecting victims. This was 40% more than in the same period in the previous year. Only 19% of the victims were able to get their money back in 2019; that is 2% less than the prior year.

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 fraudsters 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, criminals

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 fraudster's account.

Example:	The CEO of a UK-based energy company was defrauded of $243,000 when a deep fake voice pretended to be the parent company's CEO and instructed him to transfer money to a supplier. The voice sounded exactly like the parent company's CEO.

C. Breaching 2FA

Many companies and financial institutions use two-factor authentication (2FA) controls. Fraudsters use techniques like SIM swapping to circumvent the control. SIM swapping exposes weaknesses in 2FA, particularly when criminals attempt account-takeover fraud.

Example:	A fraudster visited a retail store of a mobile service provider. The fraudster reported a device (not hers) as lost. She asked the provider to activate a new SIM card with a phone number that was not hers. She had convincing identification and the store clerk activated on the criminal's device which she said was a spare phone. This enabled the fraudster to circumvent 2FA 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 and distributed denial-of-service attacks overwhelm a company's information system's resources so that it is not able to respond to service requests. The distinction between the two is that the DDoS attack is launched from a large number of other host machines that are infected by malicious software controlled by the attacker. The interesting thing about this mechanism is that the hacker doesn't actually gain access to a system, their goal is simply to take a system offline. However, there are other motives behind the attacks.

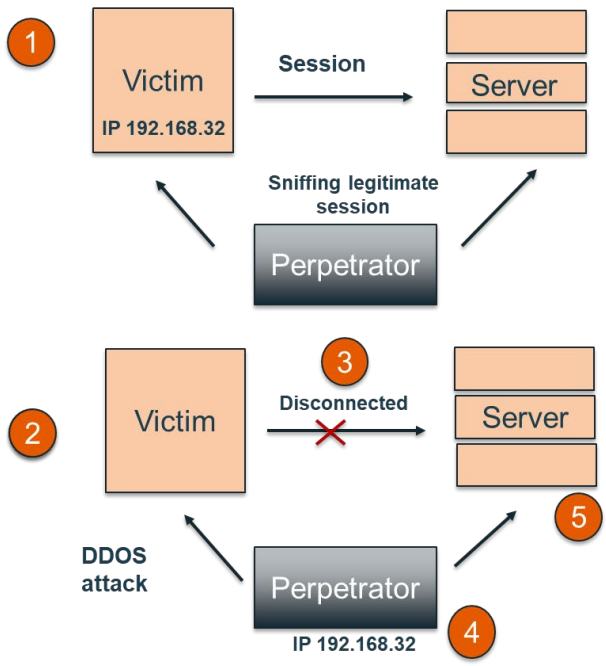
For example, if the hacker is working for a competitor taking a company's system offline could disrupt the other business and the benefit to the attacker and his employer could be real enough. However, more often the technique is used to disrupt a system so that the hacker can launch another type of attack.

1. TCP SYN flood attack

In a TCP (Transmission Control Protocol) SYN (synchronize) session initial handshake, a hacker exploits the use of the buffer space and floods the system with connection requests but does not respond when the target system replies to the requests. This causes a time out for the system while they wait for a response from the hacker's device. When the connection queue fills up the system will crash.

In this attack, an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker's device floods the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or become unusable when the connection queue fills up.

EXAMPLE



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:

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

2. Teardrop attack

This attack causes the length and fragmentation offset fields in sequential Internet Protocol (IP) packets to overlap with one another on the attacked host. When the attacked system attempts to reconstruct packets during the process and fails, it becomes confused and crashes.

3. Smurf attack

This attack involves using Internet Protocol (IP) spoofing and the ICMP (internet control message protocol) to saturate a target network with traffic. Hackers use IP spoofing to convince a system that it is communicating with a known, trusted entity. The hacker sends a packet with the IP source address of a known, trusted host instead of its own IP. This provides the attacker with access to the system.

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

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

4. Ping of death attack

The hacker uses IP packets that are over the maximum size to 'ping a target system.' Since IP packets of this size are not allowed, the attack will fragment the IP packet. Once the target system reassembles the packet, it can experience buffer overflows and other crashes.

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

5. Botnets

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

Solution: Bots can be mitigated by RFC3704 and black hole filtering.

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 hackers required payment through the US mail. As technology has evolved, payment is now generally demanded by Bitcoin or credit card. Law enforcement officials recommend that a victim refuse to pay the ransom. The malware often enters the system through phishing email.

DDoS and ransom attacks are often linked. Ransom attacks take two forms. In some instances, the cyber criminals threaten to launch a DDoS attack on an organization's site unless the organization pays a ransom fee in Bitcoin. In other instances, cybercriminals infect machines in a network with crypto ransomware that encrypts all files, then demand a ransom fee to unlock the files.

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

E. Phishing and spear phishing attacks

Phishing is where the hacker sends emails that appear to be from trusted sources with the goal of gaining personal information or convincing users to do something. It combines social engineering and technical trickery. Phishing could involve an attachment to an email that loads malware onto a computer. Phishing could appear to be a link to a website that tricks the victim into downloading malware or providing the hacker with personal information.

Spear phishing is a specific type of phishing activity. Hackers research the habits and language of the victim and craft emails that are personal and relevant. Because of this, spear phishing can be very hard to identify. Hackers may use email spoofing. In this scheme the information in the "From" section appears to come from someone known to the victim, generally someone with the authority to issue instructions. Another technique that hackers use is website cloning. The hacker copies a legitimate website and the victim enters personally identifiable information (PII) or login credentials.

Solution: Where technology is used to prevent attacks for the schemes above, phishing requires manual intervention. Here are some approaches companies can use:

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

F. Drive-by download attacks

Drive-by download attacks are a common method of spreading malware. The hacker 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 re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window.

Unfortunately, a drive-by doesn't 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.

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

G. Password attacks

Passwords are the most commonly used mechanism to authenticate users to an information system. Therefore, a hacker may try to attack by guessing passwords. Hackers will sometimes look around a person's desk if they are in the same location. Alternatively, they may ''sniff'' the connection to the network to acquire unencrypted passwords, use social engineering, gain access to a password database or simply guess. A hacker has several methods he/she can use.

- **Brute-force** password guessing – Trying passwords based on information that is known about the user such as their name, job title, hobbies, children, or pets.
- **Dictionary attack** – The hacker copies an encrypted file that contains the passwords; they apply the same encryption to a dictionary of commonly used passwords and compare the results.

H. Cross scripting attacks

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

Solution: Web developers can sanitize data input by users in an HTTP request before reflecting it back. This will make sure all data is validated, filtered or escaped before echoing anything back to the user, such as the values of query parameters during searches. They can also give users the option to disable client-side scripts.

I. Eavesdropping

A hacker can launch eavesdropping attacks by intercepting network traffic. The hacker's goal is to obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. When eavesdropping is passive the hacker finds information by listening to the message transmission in the network. Hackers can also actively eavesdrop by camouflaging themselves as a friendly unit sending queries to transmitters. In order to launch an active attack, the hacker must first gain knowledge of friendly units.

Solution: Data encryption is the best way to counteract eavesdropping.

J. Malware

Malicious software is installed in the victim's system by the hacker. It can attach itself to legitimate code and then spread. It can be hidden in useful applications or replicate itself across the Internet. There are many types of malware, some of which are described below:

- **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.
- **File infectors** attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded.
- **System or boot-record infectors** attach to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can spread to other disks and computers.
- **Stealth viruses** compromise malware detection software so that the software will report an infected area as being uninfected.
- **Trojan horses** hide in a useful program. They have a malicious function but do not self-replicate. They are used by hackers to infiltrate a system but also have another feature whereby they can establish a back door that can be exploited by the hacker.
- **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 itself across the internet, conduct malicious activity and overload email servers which can result in DOS attacks.
- **Ransomware** is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid.

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. The devices can be remotely monitored and controlled. One use to which most people can relate is Alexa. But there are many others. They can be categorized in three main 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 as presentation is loaded on a screen.**
Industrial	**Assembly line machine provides data to the plant operator on anomalies predicting when parts need to be replaced. Drones and other devices used by the military.**

These are very helpful applications. However, the Varonis Study, 110 Must-Know Cybersecurity Statistics for 2020 (Varonis Study) noted that 61% of organizations have experienced an IoT security incident. In addition, IoT devices experience an average of 5,200 attacks per month. Current studies show that there is not a lot of risk on the consumer front but there are risks in enterprise and industrial application including device discovery, automation and authorization, and infiltration due to DoSs attacks by bots and other malware.

L. It's also a people problem

Hackers 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. Hackers 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 hacker can use to gain access into the system. According to Verizon's annual Data Breach Investigations Report, social engineering attacks, including phishing, are responsible for 93% of successful data breaches. Hackers generally use social engineering to gain access to passwords, bank information or a computer so they can install malware to give them access to a lot more. Knowledgeable aware people are the antidote to social engineering. Trust takes a back seat when it comes to information security. The best question to ask is: "How do I know that the person I am communicating with by email, text, website or online interactions is really who they say they are?"

When the hacker manages to obtain access to one person's password, they have access to that person's contact list. They can then use the email account of the first victim to send emails to the person's contacts. Links can be embedded in the emails and if it appears that the email is a trusted source then clicks on the link give the hacker a second victim. The email could also have a download of music, movies or documents with embedded malware. Even hovering over the email address to see if it is legitimate may not be completely effective since hackers can also camouflage their true email addresses with overlays. Hackers frequently impersonate companies and the emails look legitimate right down to the logos and key words that the bank might use. According to Webroot data, financial institutions are the most often impersonated.

Hackers will ask for donations, present an issue and ask the victim to validate information by providing information in a form or clicking on a link, offer something free, respond to a question the victim never

asked, claim that the victim is winner of some prize or pose as a co-worker, boss, company executive, etc. These techniques find their way into company sponsored email accounts as well as personal ones.

Solutions:

- Slow down. Nothing is that urgent that it should not be carefully reviewed.
- Ask for oral verification even if it slows down the process. Call the sender and ask.
- Go straight to the website of the financial institution purporting to be the sender in a fresh browser and see if there are any messages waiting there.
- Delete any requests for financial information or passwords.
- Scams come in the form of offers to help, e.g. restore credit scores, refinance a home, etc. Delete them.
- Secure computing devices with anti-virus software, firewalls, email filters and update them regularly.
- Companies should train employees and penalize them for disregarding policies and procedures on information security.

Example 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 hacker 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:

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

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: • WhatsApp Messenger; • Pokémon GO; • WinZip Utilities; • CamScanner Productivity; • Plex; • WeChat; • Facebook Messenger; • eBay Kleinanzeigen; • NetEase News; and • Device Alive. The biggest issues identified were sending SMS messages or sensitive data without encryption, accessing address books and cameras without permission, 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

In October 2018, the SEC issued a report on an investigation into nine companies that experienced losses of almost $100 million due to cyber fraud. The techniques used by the fraudsters are common. Company personnel received spoofed or compromised electronic communications from outsider sources causing them to transfer funds to the bank accounts of the fraudsters.

One of the companies cited in the report made 14 electronic transfers based on fictitious emails received from fraudsters masquerading as company executives. Another company paid 8 invoices over several months to what they believed were legitimate vendors. However, the routing instructions had been changed to a fraudster's bank account.

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.

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

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

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 fraudsters. 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 only 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 robust cyber fraud risk assessment process;
- Establishing more stringent cybersecurity policies and procedures;
- Performing scenario analysis including how management could override controls;
- Identifying key controls to prevent improper disbursements or accounting errors from cyber fraud focusing on payment requests, authorizations and disbursement approvals especially for large, nonsystematic, time sensitive or foreign transactions;
- Identifying key controls over changes to vendor disbursement processes;
- Evaluating the design and test controls;
- A cyber fraud diagnostic from an entity specializing in this service;
- Training personnel and penalizing those who violate the controls even through carelessness; and
- Monitoring activities with data analytic tools for potential improper disbursements.

Deloitte published this list of General IT Controls in its October 30, 2018 edition of *Heads Up*.

Type	Purpose	How it Works
Multifactor Analysis	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 hacker from accessing a hosted email solution that would then be used by the hacker 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.

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?

SAS No. 142, *Audit Evidence*

SAS No. 142, *Audit Evidence*

Learning objectives

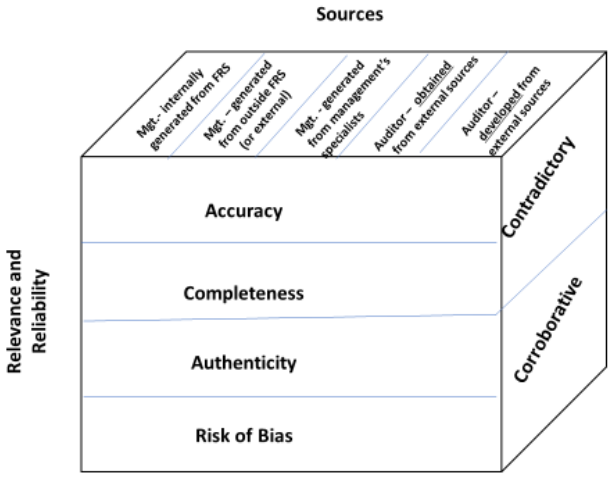
Upon completing this chapter, the reader will be able to:

- Understand the important characteristics of audit evidence;
- Understand the evidence needed to support the use of newer technologies; and
- Implement SAS 142, *Audit Evidence*.

I. Introduction

AU-C 500, *Audit Evidence*, has not had significant revisions since 2005 even though the standard was clarified in 2011. Much has changed since that time as the size and complexity of audited entities has increased and technology and its use by auditees and auditors has progressed. In 2017 the AICPA launched a project to assess whether it was time to revise the standard in light of these issues. In addition, the AICPA's audit quality initiative identified issues related to lack of professional skepticism. In a separate project the IAASB was also seeing these issues.

The standard not only addresses emerging technologies but also discusses professional skepticism, management specialists, and audit documentation. Its primary focus is to assist the auditor in assessing whether sufficient and appropriate audit evidence has been obtained when the information is attained from sources not available when the earlier standard was issued. The ASB presents attributes and factors for auditors to use in evaluating audit evidence no matter the source or the way the auditor obtained the information (including the use of automated tools and techniques). These attributes and factors will be discussed throughout the chapter. Although the standard discusses and provides examples of newer technologies and methods, they are not described in detail.



SAS 142, issued in July 2020, is effective for periods ending on or after December 15, 2022.

II. Definitions

The proposed SAS contains four definitions that set the foundation for this standard:

1. **Appropriateness (of audit evidence)** – The measure of the **relevance and reliability** of audit evidence. Appropriateness relates to the quality of the audit evidence.
2. **Sufficiency (of audit evidence)** – The measure of the **persuasiveness** of audit evidence. The persuasiveness of audit evidence necessary is affected by the auditor's assessment of the risks of material misstatement. Sufficiency relates to quantity.
3. **Audit evidence** – Information used by the auditor in arriving at the conclusions on which the auditor's opinion is based.
4. **External information source** – An individual or organization external to the entity that develops information used by the entity in preparing the financial statements or used by the auditor as audit evidence, when the information is available for use by a broad range of users.

When information has been provided by an individual or organization acting in the capacity of management's specialist, service organization, or auditor's specialist, the individual or organization is not considered an external information source with respect to that particular information.

III. Attributes and factors – Relevance and reliability

During the financial statement audit the auditor accumulates audit evidence to support his/her opinion on the financial statements. The term *sufficient appropriate audit evidence* is not new. The SAS explains that the attributes and factors in the cube above are to be evaluated to determine if sufficient appropriate evidence has been obtained. The auditor should evaluate the information to be used as audit evidence for relevance and reliability. This includes the source and whether it corroborates or contradicts assertions in the financial statements.

The front of the evidence cube discusses the important factors of **relevance and reliability**. The auditor considers the attributes: accuracy, completeness, authenticity, and bias.

A. Relevance

Relevance refers to the logical connection with an assertion under consideration. The factors that affect the relevance of information are:

- The objective of the procedures to be performed as well as the assertions;
- The account balances, classes of transactions or disclosures to which the information relates; and
- Period of time to which the information relates.

Example:	An auditor was testing accounts payable. She considered the following: • **Objective of procedures and account balance** – to test the existence or valuation of accounts payable. When testing existence, the auditor would test the recorded amount of accounts payable. The auditor could confirm accounts payable and reconcile the confirmations to the recorded balance and vendor statements. This would be relevant audit evidence. • **Objective of procedures and account balance** – to test the completeness of accounts payable the information discussed related to the recorded balance would not be relevant. However, information coming from subsequent disbursements, unpaid invoices, unmatched receiving reports, or supplier's statements would be.

When looking at an account balance the auditor has to pay careful attention to the assertions. For example, in evaluating marketable securities, a document (electronic or paper) may provide good evidence for an asset when it comes from an external source like a financial institution. On the other hand, a record viewed on blockchain may not be quite as good evidence unless the reliability of the blockchain has been confirmed. The auditor also needs to consider ownership and valuation through other tests. The evidence that a security exists is not the only consideration. A confirmation or statement does not provide information about valuation or ownership.

External confirmations can be very useful for more than account balances. The auditor might request confirmation of terms and conditions or even the absence of other accounts. For example, a bank confirmation will provide a balance (existence) but can also provide evidence of additional accounts that might be open or liabilities that the entity may or may not have disclosed.

Example:	An audit senior was testing revenue and accounts receivable. She sent out confirmations to the largest accounts to determine whether the balances existed. She also evaluated subsequent receipts to evidence the amount being paid and that it existed at the balance sheet date. Confirmations and subsequent receipts are also supportive evidence for rights and obligations. The audit manager asked her to go back and perform a test of valuation by looking at the aging report and evaluating how many of those balances were paid. She also asked her to look in hindsight to determine if the allowance for bad debts was adequate in the prior year. Finally, she asked her to consider the aging of the receivables given the historical knowledge of the client's ability to estimate as well as any current conditions identified during the risk assessment process. These procedures, however, did not test completeness of revenue and receivables. The auditor generally tests debit balances (receivable) for overstatement and credit balances (revenue) for understatement. Analytical procedures are very helpful in this regard. The manager helped the senior auditor to develop an appropriate analytical procedure.

B. Reliability

The reliability of information is affected by these attributes:

- Accuracy;
- Completeness;
- Authenticity; and
- Risk of bias.

1. Internal controls

The auditor's judgment and professional skepticism play a significant role in his/her consideration of reliability. The auditor should consider that information is more reliable when controls over its accumulation, preparation, and maintenance have been tested. Note that this information could be tested by the external auditor or if the information is accumulated, prepared and maintained at a service organization, then a combination of the service organization's auditor and the user auditor (complementary user controls).

Evidence accumulated in testing internal controls could be derived from written records such as board of director meeting minutes, observation by the auditor, evidence in documentary form such as an approval of an invoice, or orally. It is always appropriate to obtain oral explanations for how a control is performed. Corroboration of an assertion by an employee or by an internal or external third party is helpful. But oral evidence alone is not as persuasive as review of documents or observation.

Tests of controls are required when information is only available in electronic form or in cases where substantive testing alone would not provide sufficient evidence.

2. Accuracy and completeness

Evidence should be tested for completeness and accuracy. Before choosing a sample, the auditor should reconcile the population from which the sample is chosen to the general ledger to ensure completeness. Tests of controls also provide evidence about completeness.

An auditor may also use information developed outside of the financial reporting system as audit evidence. The auditor could use the entity's performance measures for substantive analytical procedures (SAP). To ensure that the report with the performance measures is accurate and therefore precise enough to use in an SAP, tests of controls or tests of accumulation of information could be needed.

Example:	The sales department at a client provided an auditor with a scanned version of an executed sales contract. Since the contract was not an original the auditor considered whether it would be more effective and efficient to confirm key terms with the third party or test the operating effectiveness of internal controls around the operating effectiveness of the execution of the original contract and maintenance of the scanned version.

3. Authenticity

Auditors are required to consider the possibility of fraud in a financial statement audit. Auditors are not authentication experts but if there is suspicion that a document may be fraudulent the auditor will address this by corroborating the evidence by other means.

Example:	An auditor was aware that the client scanned or obtained many source documents electronically in order to save storage space and reduce the entity's footprint. During the audit of investments, she noted that the investment statement looked as if it could be altered. Since investments were not material to the balance sheet and were deemed to be of less risk since they were all publicly traded, the auditor generally obtained the end of the year statement and used it for testing rather than confirming the balance. The auditor asked the controller to sit with her and she went to the client's portal to obtain the source document herself. She downloaded the document and compared it to the client's copy. She discovered that one of the balances at the bottom of one page was altered so that the balance of investments was lower by $10,000. This caused her to perform further procedures.

4. Risk of bias

The risk of bias is present in all audits, particularly as it relates to estimates. There are two forms of bias, management bias and auditor bias.

5. Management bias

There is a higher risk of management bias when information comes from internal sources. There are several considerations here:

- The ability of the entity to influence the external information source;
- Management's selection of information so that it "proves" management's assertions; and
- Management's unknowing use of information from an external source that is biased.

Example:	An auditor was considering an estimate for the valuation of alternative investments prepared by the client. The client prepared a memo supporting each one of the investments citing industry information on rates of return, earnings of the companies in venture funds, and the views of investment fund managers. The partner on the engagement realized that this estimate had more risk of bias either because the client chose reports that were favorable to the investments to support the valuation or because management did not adequately challenge information provided to them by the fund managers. The auditor realized a high degree of skepticism and verification of sources would be necessary to reduce the risk of bias.

6. Auditor bias

Auditor's bias may actually be more challenging to address. The auditor's judgment may be hampered by:

- **Availability bias** – The auditor chooses information that is easily retrievable as being more likely, more relevant, and more important for a judgment.
- **Confirmation bias** – The auditor looks for information that is consistent with initial beliefs or preferences.
- **Overconfidence bias** – The auditor overestimates his/her ability to make accurate assessments. For example, in the case of complex financial instruments the auditor does not seek outside assistance to assist in evaluating an assertion.
- **Anchoring bias** – The auditor assesses an account balance by starting with a number and not adjusting far enough away from the initial value.

Example:	An auditor was performing an SAP on payroll during an audit. He began with the prior year balance of payroll expense, divided it by the prior year number of employees and multiplied it by the current year number of employees. He also adjusted the resulting balance for the average raise received by the employees. He concluded on the workpaper that the amount of the client's payroll balance was "reasonable" although his calculation was off by twice the entity's materiality. Since there was a significant deviation from the general ledger balance, the manager on the engagement suggested he talk to the human resource director to determine if the larger raises were given to more highly compensated people. He also identified the salaries of the new hires to compare them to the average salary calculated in the SAP.

C. Sources of evidence

The top of the evidence cube identifies these five sources of evidence:

- From management – Generated internally from the financial reporting system;
- From management – Generated outside the financial reporting system, including from sources external to the entity;
- From management – Obtained from management's specialists;
- Auditor – Obtained from sources external to the entity; and
- Auditor – Developed from sources internal or external to the entity.

The auditor may use one or more of the sources identified above.

Example:	An auditor of an entity with a defined benefit pension plan was evaluating audit evidence used by management in their estimate of the accumulated benefit obligation. Some of the information involved in the calculation was generated internally from the financial reporting system. Other information was provided by an actuary, who was considered one of management's specialists. The auditor tested that information by obtaining, understanding, and testing the accumulation of data provided to the actuary by management. Then the auditor tested the information provided by the actuary using the audit guidance in AU-C 620, *Use of an Auditor's Specialist*, that is relevant when management uses a specialist.

1. Internal information – Data analytics and methodologies used in auditing

In the past much of the internal information requested by an auditor consisted of source documents such as checks, invoices, contracts, ledgers, journal entries, spreadsheets, cost allocations, computation, reconciliations and disclosures. And most of it was in paper form. With the many advances over the years in information technology, a significant amount of evidence is now in electronic form either having been transmitted to or from the client electronically or scanned in when received. Other internal forms of data might come from outside accounting in the form of sales, marketing, or other system-generated reports.

Auditors traditionally performed manual testing of internal controls and substantive testing along with straightforward analytical procedures using computer aided audit techniques. However, as companies and their systems and processes have become more complex and clients embrace newer technologies, auditors are, in many cases, expected to do the same.

Audit data analytics is described as a technique that analyzes patterns, identifies anomalies or extracts information from data through analysis, modeling or visualization. Some of the data used in these tests is financial and some is operational. For example, if an auditor wants to test retail sales by regression

analysis, he/she may obtain information about square feet in the retail store and sales prices from management (internal) and changes in the consumer price index (external).

Typical uses of the automated techniques in the past have been to:

- Foot journals and ledgers to determine accuracy;
- Choose journal entries;
- Scan data to identify anomalies;
- Identify samples for testing; and
- Perform regression analysis.

Auditors may want or even need to be able to perform more sophisticated data queries and then portray the data visually so that patterns can be seen more easily. Data analytics can be used effectively for those purposes. This adds value to the auditor's work and also adds value to the client. These more sophisticated analytics are not without risk. If the data is not relevant and reliable the test will not provide appropriate evidence. Auditors need to consider the need for tests of controls or tests of accumulation of information to provide evidence of reliability of the data used. They also need to be skilled in understanding the client's business to ensure that the right data is used. They also need to be skilled in the application used to perform the test.

Audit data analytics is by far the most widely accepted of the newer audit methodologies. SAS 142 mentions other techniques that can be used by auditors but does not go into detail describing them. These are briefly described here:

- **Artificial Intelligence** (AI) is a set of algorithms that perform work that traditionally requires human intelligence. The algorithms are created to classify, analyze, and draw predictions from data. There are a number of different AI applications that involve acting on data, learning from new data, and improving predictability over time. AI can be simple or very complex. Some of the simpler examples are Google Search, Alexa, Siri and other personal assistants, and image recognition software.
- **Machine learning** is a type of AI. Machine learning feeds a computer with data and uses statistical techniques to help it "learn" how to get progressively better at a task. For example, if a user feeds a computer with large amounts of data on sales and advertising dollars spent, machine learning is used to see the patterns in data and make predictions of future sales based on dollars spent. Another useful application is the use of computer vision to read and analyze complex contracts.
- **Robotic process automation** is a technology application that automates routine business. An entity can use this tool to capture and interpret applications for processing transactions, manipulating data, triggering responses and communicating with other digital systems. Applications of RPA can be very simple. For example, a robot can be created that generates an automatic response to an email. Some applications take routine business processes and automate them. For example, RBA can be constructed to take an electronic invoice, match it to a purchase order and receiving documents and either approve or reject it until discrepancies can be resolved. Auditors can use RBA to streamline repeatable processes as well.
- **Remote observation** tools such as drones can be used for many applications such as counting inventory in difficult to reach places.

Automated techniques may also be used both as risk assessment procedures and as substantive procedures concurrently if the objectives of both types of procedures are achieved.

2. External Information

External information can be more challenging to test since the auditor may have less access to determine reliability and may be biased to believe that since the information is external to the client it is automatically reliable.

As defined earlier in this chapter, external information sources develop information that is available for use by a broad range of users. An external source is **not** a management's specialist, a service organization, or an auditor's specialist. External sources could be pricing services, governments, central banks, stock exchanges, media, or academic journal.

The auditor may consult these sources to obtain:

- Prices and pricing-related data;
- Macroeconomic data, such as historical and forecast unemployment rates and economic growth rates, or census data;
- Credit history data;
- Industry-specific data, such as an index of reclamation costs for certain extractive industries or viewership information or ratings used to determine advertising revenue in the entertainment industry;
- Mortality tables used to determine liabilities in the life insurance and pension sectors; and
- Documents or records on websites or in databases or distributed ledgers.

An entity or individual acting as a specialist or service organization may fill more than one role and professional judgment may be necessary to determine the capacity in which the person or organization is acting at a particular time.

Example 1:	Actuaries are frequently involved in valuations, for example pension liabilities or claims payable. Acting in this capacity the actuary is not an external source. But when actuarial firms publish data on mortality or other such information they are functioning as external sources.

Example 2:	Certain valuation specialists use models such as Black Scholes to estimate the valuation of derivative instruments since there is no observable market. If that entity is engaged to provide specific valuations and gives information to management for use in the entity's financial statements, then that entity is functioning as management's specialist. However, if the valuation company prepares information and provides it to the public and the entity takes and uses that information in its own estimation methods then the company would be considered an external source.

The auditor will need to consider the relevance and reliability of the information no matter whether it was obtained by management or the auditor. With external information the auditor considers:

- Information about the external information source or the preparation of the information by the external information source;
- Audit evidence obtained through designing and performing further audit procedures;
- Why management or, their specialist uses an external information source, and how the relevance and reliability of the information was considered so that the auditor can consider those attributes or variables;

- The nature and authority of the external information source;
- The ability of management to influence the information obtained, through relationships between the entity and the external information source;
- The competence and reputation of the external information source with respect to the information;
- Past experience of the auditor with the reliability of the information provided by the external information source
- Evidence of general market acceptance by users of the relevance or reliability of information from an external information source for a similar purpose to that for which the information has been used by management or the auditor;
- Whether the entity has in place controls to address the relevance and reliability of the information obtained and used;
- Whether the information is suitable for use in the manner in which it is being used;
- Alternative information that may contradict the information used;
- Nature and extent of disclaimers or other restrictive language relating to the information;
- Information about the methods used in preparing the information and how the methods are being applied including, where applicable, how models have been used in such application, and the controls over the methods: and
- Information relevant to considering the appropriateness of assumptions and other data applied by the external information sources in developing the information obtained.

Should the auditor have doubts about the reliability of the information he/she may decide to perform a comparison of the information obtained from the external source with information obtained from another independent information source. The auditor could also consider obtaining an understanding of management's controls over the reliability of external information and perhaps even test them.

If the auditor does not have a sufficient basis to consider the relevance and reliability of information from an external information source, it could mean that there is a scope limitation. If alternate evidence cannot be found, then the opinion may have to be modified.

3. Evaluating information used as audit evidence

Audit evidence can take many different forms depending on how it is accumulated. Different forms of evidence include:

- **Oral evidence** – Oral inquiries are made during the audit to both internal sources such as management or external sources such as attorneys. Inquiries are often the place the auditor starts in developing his/her understanding of the entity and its environment including internal control. Oral inquiries should be backed up with other forms of evidence.
- **Visual information** – Auditors use observation in risk assessment procedures such as understanding an entity's internal control. Observation is also used in connection with physical inventories. For example, an auditor could observe a message that appears on client personnel's computer screen evidencing restricted access to an IT application. Drones or video technology could be used as remote observation tools to facility inventory observations.
- **Paper documents** – Auditors will probably continue to see paper documents as forms of evidence for the foreseeable future until such time as entities embrace electronic forms of

transmission. For example, executed contracts, leases, loans, and written confirmations are often presented to the auditor as paper documents.

- **Electronic information** – Many documents that at one time were presented to the auditor in paper form are now electronic and this trend will continue. Paper documents such as a paper contract can be scanned. Alternatively, some documents are executed electronically using Docusign or a similar application.
- **Data** – Data that is stored in the entity's IT system or obtained from an external source may be either manually input into the system or electronically generated. For example, there is often an electronic interface between an entity and a service organization which is used to transmit data.
- **Client records** – The auditor also inspects records that may be in paper form such as accounting entries, checks, electronic fund transfer confirmations, invoices, contracts, ledgers, journal entries, spreadsheets, cost allocations, reconciliations, and disclosures.
- **Information from published sources** – In performing procedures like regression analysis the auditor may use information from trade groups or government agencies often in combination with information from management.

Example:	An auditor wanted to perform a predictive substantive analytical procedure on cost of sales of certain products. She obtained an index of product cost increases from a trade group and used that along with information provided by management on square footage of retail space and historical margin information to predict cost of sales by regression analysis.

D. Corroborative or contradictory information

The other side of the evidence cube illustrates the effect of corroborative and contradictory information. AU-C 330 states that when the auditor forms a conclusion about whether sufficient evidence has been obtained, he/she should consider **all** the evidence no matter if it corroborates or contradicts the assertions. Contradictory and corroborative information is considered together not in isolation. Sometimes the absence of information is used by the auditor and constitutes evidence.

Example 1:	An auditor was auditing a financial institution with an extensive portfolio of loans secured by real estate in one geographic area. The auditor obtained industry information about the market where the real estate was located that contradicted the appraisals management gave the auditor to support the value of the collateral. The auditor had to perform additional procedures to reconcile the difference.

Example 2:	An auditor was evaluating information related to management's assertions about the recorded balance of the entity's provision for warranties for a certain product. She inquired of the people handling returns of product and asked to see reports to determine the amount of sales returns during the period. She noted an absence of sales returns of the product in question which supported management's assertion about the completeness of the provision for warranties.

E. Audit procedures

The auditor obtains audit evidence by performing risk assessment procedures, tests of controls (when required or when the auditor chooses to perform them) and substantive procedures which take the form of tests of details and SAPs.

An auditor may use manual techniques or automated techniques such as audit data analytics, to process, organize, structure, or present data in a given context in order to generate useful information that can be used as audit evidence.

These days some information may be available only in electronic form or only at certain points or periods in time. This can impact the auditor's testing strategy. If the entity's data retention policies are not long enough the auditor may need to request that the client retain certain information during the year so that it can be used either at a later time or the auditor may choose to perform procedures when the data is available. Other electronic information such as records maintained on a blockchain is available on a continuous basis during the audit. This makes it easier for auditors to use audit data analytics or artificial intelligence to obtain information about transactions on a real-time basis.

Other audit procedures performed on information may include inspection, observation, confirmation, recalculation, reperformance, analytical procedures, and inquiry. Auditors use the procedures they believe will be most effective and efficient. Some of these procedures lend themselves to either manual testing or using automated tools. Inquiry is a very important part of auditing and can lead to further testing in some areas, but auditors should be aware that inquiry alone does not provide sufficient appropriate audit evidence.

1. Controls over information to be used as audit evidence

As noted earlier when information is transformed from its original state, whether its scanned, filmed, digitized or transformed by other means, the data may lose its reliability. Accordingly, the auditor may need to perform additional audit procedures to address the reliability of the data such as inspection of the original documents or tests of internal controls over the transformation and maintenance of the information.

Testing internal controls becomes even more important when the information is electronically initiated, recorded, processed, or reported and is only available in electronic form. Here the sufficiency and appropriateness of the evidence usually depends on the effectiveness of controls related to data accuracy and completeness. When the source documents are electronic there is more risk that the documents could be inappropriately initiated or altered, and the fraudulent activity remain undetected.

2. Inspection

Auditors have always performed physical inspection of assets and documents. Over the years, things have evolved so that the documents are now, in large part, in electronic form. An automated technique that is being used currently is artificial intelligence programs that use text recognition programs to examine documents. These programs identify items for further audit consideration.

3. Observation

Observation consists of looking at a process or procedure being performed by employees. One example is the observation of inventory. Where this can be a manual process, automated tools and techniques such as use of drones not only assist but can add accuracy to a process.

Example:	An audit firm had a client with a significant amount of inventory in several warehouses. Management began using the drones to try to solve the continued differences between the perpetual inventory and the general ledger. They used drone technology to do cycle counts every month. The drones scanned the bar codes and took video which enabled management to understand where bar codes were damaged and needed to be replaced, identified issues earlier so they could be corrected, and cut down on manual errors made when humans performed the counts. In addition, it provided better coverage since the drones could do accurate counts in difficult to reach places. The client permitted the auditors to observe the use of the technology for counts during the year and also permitted them to use the technology to take test counts themselves.

4. External confirmation

An external confirmation is a direct response knowingly provided to the auditor by a third party (the confirming party).

5. Recalculation

Recalculation consists of testing the mathematical accuracy of information. Recalculation may be performed manually or using automated tools and techniques. Auditors have been using technology to recalculate reports as well as foot the general ledger.

Example:	An auditor wanted to recalculate gross margin for each product sold to use in an analytical procedure. He was able to use automated tools to make those calculations. The process saves time and improves accuracy.

6. Reperformance

Reperformance involves the independent execution of procedures or controls that were originally performed as part of the entity's internal control.

7. Analytical procedures and use of audit data analytics

Auditors frequently use analytical procedures to test revenue and expense accounts as well as some balance sheet accounts. They are also used in risk assessment to identify anomalies in data that may point to a significant risk. When used as a risk assessment procedure a visual of transactional detail can provide auditors with an illustration of the volume and dollar value of a population. If the analytic can provide sufficient precision, the same analytic could be used for both risk assessment and substantive testing. The auditor may also use audit data analytics to obtain evidence about the effectiveness of the entity's internal control.

Example 1:	An auditor wanted to test automated controls over sales invoices. The system was supposed to identify errors when the invoices were out of sequence or when duplicates existed. Data analytics were used to look for these issues. Not only did this procedure test an automated control, it also provided information about the completeness of invoices issued during the period.

Example 2:	An auditor was testing entity level internal controls and obtained information from the internal audit department to support the entity's monitoring activities. He decided that the information would be good to use in a substantive analytical procedure. Before using it, the auditor evaluated the information to ensure that it was sufficiently detailed and precise to use for the secondary purpose.

Example 3:	An auditor wanted to use audit data analytics as a risk assessment procedure to look for unusual transactions or events and amounts, ratios, and trends that might indicate an area of higher risk. She found it easier to spot issues by looking at visualizations of transactional detail. She prepared an analytic of sales data displayed as a visual highlighting per unit values and number of items in a population. Although the procedure was primarily performed as a risk assessment procedure, the auditor determined that it yielded sufficiently precise information and the output could be used in a substantive analytical procedure as well.

Auditors scan the general ledger to look for significant or usual items to test. Auditors can use programs to perform data analytics that will help them extract data that meet certain parameters. This could mean transactions ending in round numbers or transactions that are right above a dollar value required for additional approval, etc. The auditor can use these tools to run Benford's law, an algorithm that predicts anomalies in a population based on the expected frequency and placement of numbers in a monetary transaction.

8. Inquiry

Inquiry consists of seeking information, both financial and nonfinancial, from knowledgeable persons within the entity or outside the entity. Auditors use inquiry throughout the audit, coupled with other audit procedures. Evaluating responses to inquiries is an integral part of the inquiry process. Corroboration helps to confirm what one person has told the auditor. Often this is used in an understanding of internal control.

F. Audit applications

As noted earlier, audit data analytics can be used in risk assessment procedures, tests of internal controls, and substantive analytical procedures. To get the most out of the applications it is important to be methodical. There are two major risks with performing analytics as audit evidence. The first is that the data is not relevant and reliable and the other is that the procedure is poorly designed. The risk is relying on the results of procedures with one or both of these flaws.

To summarize the steps to help reduce the risks with performing analytics as audit evidence:

Step 1: **Flowchart the process that is involved**. It will be important to understand where the data comes from and how it is laid out in the information system.

Tools include flowcharting software sources, such as Tableau Public, RapidMiner, Qlicksense and even Excel.

Step 2: **Choosing and extracting the data.** This step is already being performed in many audits. There are many products on the market that use a variety of scripts that can be adapted to various data formats. And there is also a variety of data extraction software products. Providers have not standardized around the AICPA's Audit Data Standards (ADS) or any other common standard.

Tools include Capterra, ACL, Caseware, IDEA, SAP, Oracle.

Step 3: **Understanding the population.** It is important to understand the nature, distribution, and the limitations of the population to be tested. This helps the auditor to choose the

right analytic technique. This also includes whether there is a problem with data availability. For example, does the population contain a complete set of data in all fields or is data missing?

Step 4: **Exploratory data analysis.** The AICPA is stressing the concept of data visualization and the significant role it plays in decision making. By creating visuals, the auditor can identify where to focus attention on the highest risks.

Example 1:	An auditor obtained a data set for revenue and expenses to try to understand why revenue increased $2.8 million and expenses decreased $5.3 million. He drilled down into the data to see which sources of revenue had the most significant increase noting that it was service revenue. He was also able to drill down and determine the specific types of service expenses that declined. This helped him to focus on areas where there might be risk so he could make further inquiries of the client and devise a testing plan. The visuals in the form of graphs showing monthly revenue for the various large revenue streams helped to see the issues very quickly.

Example 2:	An auditor was evaluating the allowance for uncollectible accounts receivable. She was able to determine, through data extraction software, which receivables were open and which had been cleared after year end. The software allowed her to do this by aging category. The next step was to see how the balances had cleared. She was able to drill down and determine how much cleared through payments to the bank and how much cleared due to credit memos. The use of graphs and bar charts was very helpful in pinpointing the fact that credit memos spiked right at the end of the period. She looked at the data further and was able to see who initiated the credit memos. This provided her with some very useful information in her risk assessment.

Step 5: **Choose methods and approaches.** There are many methods and approaches that can be used to analyze data. They come in three basic categories: mathematical and statistical methods; methods based on artificial intelligence and machine learning; and visualization and graphical methods and tools. These can be used as audit techniques and are also used by clients to manage their businesses.

Mathematical and statistical methods	**Methods based on artificial intelligence and machine learning**
Descriptive analysis - Looks at data and analyzes past events for deciding how to approach the future. ***Possible application*****:** Current expected credit losses.	AI tools use advance algorithms and machine learning to predict activity and **manage business processes** such as projecting inventory levels, managing cash flow needs or enhancing monitoring and other activities in internal audit. ***Possible implication for auditors:*** If clients use AI to execute orders and payments based on, for example, food and beverage usage at a customer site, auditors will need to understand the technology behind it since these transactions flow into the general ledger.

Regression analysis - Allows modeling the relationship between a dependent and independent variable. ***Possible application:*** Predicting account balances. Anomalies are identified for investigation. This is one of the most popular forms of data analysis.	**Smart contracts** - A smart contract is a computer code running on top of a blockchain containing rules where the parties to the contract agree to interact with each other. This facilitates, validates, and enforces the performance of an agreement or transaction. ***Possible implication for auditors:*** Auditors will need to determine where smart contracts are used and whether they might represent key internal controls. For example, a retailer might engage in smart contracts with a supplier to ensure quality goods. Goods could be rejected if in the transport of perishable goods, the temperature of the refrigerated unit fluctuates a certain number of degrees outside a threshold.
Dispersion analysis - Is the spread to which a set of data is stretched. It shows how extended a data set is. It shows the variation of things among themselves and the variation around the average value. ***Possible application:*** Graphically presenting the changes in sales by month for various types of products to see where the variation lies for investigation.	AI can be used to **read contracts and abstract key words**. This is helpful to an auditor in situations where the client has numerous leases or other documents that the auditor must analyze.
Discriminant analysis - Very powerful tool that utilizes variable measurements on different groups to separate them into categories. ***Possible application:*** Classification of customers into groups – slow payers/quick payers, high volume/low volume.	

Step 6: **Confirming data analysis and finding outliers.** Once the risk has been identified the techniques above could be used to focus on areas of interest and unusual items investigated.

Step 7: **Evaluating results.** The audit by exception approach as discussed above is very useful in targeting high risk areas. Auditors may not feel as comfortable with this approach as they do with traditional samples. If the data is clean, valid and complete and the test properly constructed the auditor may evaluate .15% of the population but it is targeted toward the items that are outliers whereas in a sample of 60 items none of them may be outliers. It is important to remember that when sampling theory was created, every test was performed manually.

G. Documentation

Audit documentation is very important in all audits but particularly where new audit techniques are used. It is highlighted by the AICPA as an important component of SAS 142. However, AU-C 230 was not amended as a result of the standard.

As in all audits, the auditor should prepare audit documentation that is sufficient to enable an experienced auditor, having no previous connection with the audit:

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

- The identifying characteristics of the specific items or matters tested;
- Who performed the audit work and the date such work was completed; and
- Who reviewed the audit work performed and the date and extent of such review.

Abstracts or copies of significant contracts or agreements should be included in the workpapers. 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.

Discussion question:

SAS 142, *Audit Evidence*, includes clarifying language to assist the auditor in incorporating new technologies into the audit process. One of the techniques that is most widely thought of as viable for both small and large firms is audit data analytics. Other newer techniques are the use of artificial intelligence to read contracts and drones for making observations.

What do you or your firm believe are the benefits and risks to incorporating more technology into audits?

Using Audit Data Analytics

Using Audit Data Analytics

Learning objectives

Upon completing this chapter, the reader will be able to:
- Understand the methodology for using audit data analytics; and
- Perform a predictive test as a substantive analytical procedure.

I. 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.

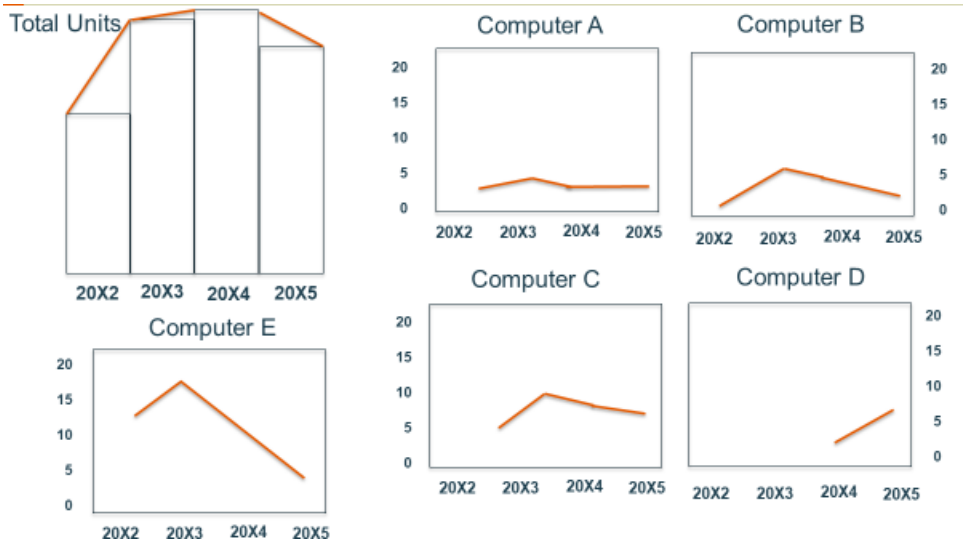
A. Preliminary analytical procedures

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. Examples of analyses that can be performed are:

- Comparison of account balances with budget and prior-period amounts;
- Analysis of changes in revenue during the current period based on statistical data;
- Payroll expense divided by number of employees;
- Other expense fluctuations from prior year; and
- 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.



1. 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% of the time. The number 2 would be the leading digit in a string of numbers 17.6% 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.

2. Documentation

For preliminary analytical procedures, the auditor should document:

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

Note that preliminary analytics were never meant to be an index to 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%

B. 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:

- Given the assertions to be tested, how suitable is an SAP?
- How reliable is the data that will be used to develop the expectation?
- Will the expectation be sufficiently precise at the desired level of assurance?
- What is the amount of unexplained difference that will be acceptable to the auditor?
- 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 numbers 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 6 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 amounts' differences between the expectation and recorded amounts of over 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 he/she does not wish to perform other substantive tests, he/she must consider the effects both individually and in the aggregate of misstatements (known and likely) that are not corrected by the entity.

1. 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 form an expectation	• 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.

2. Six step method to perform an SAP

The 6 steps in performing an SAP follow.

Step 1: Form the expectation.

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

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

- Systems with reliable controls produce more reliable expectation.
- Use external data for a more reliable expectation.
- Nonfinancial data or data subjected to auditing procedures produces a more reliable expectation (attribute testing of accumulation of information).
- Testing internal controls should be considered.
- 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, he/she will compare the expectation to recorded amounts. Differences from expectation can be due to:

- Misstatements;
- Inherent factors that affect the account being audited; and
- Difference due to factors related to the reliability 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 he/she 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 he/she does not wish to perform other substantive tests, he/she must consider the effects both individually and in the aggregate of misstatements (known and likely) that are not corrected by the entity.

II. Example: Substantive analytical procedure

A. 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.

1. 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, she 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 her expectation assuming:

- No significant events or accounting changes occurred except store openings;
- Industry and economic factors are stable; and
- 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 4 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%**

- The auditor expected a higher gross margin for those stores selling gasoline. (TEST EXPECTATION MET)
- The gross margin should be more consistent for the stores that sell gas than those that do not. (TEST EXPECTATION MET)
- 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.
- 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.

2. 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. She 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	18,942,132	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 her next steps.

Discussion questions:

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