

CHECKPOINT LEARNING

Contact us at: 2395 Midway Rd., Carrollton, TX 75006
checkpoint.learning.cpecustomerservice@tr.com
800.431.9025

CPE NETWORK

ACCOUNTING & AUDITING REPORT

SEPTEMBER 2022

VOLUME 35, ISSUE 8

EXECUTIVE SUMMARY 1

EXPERT ANALYSIS AND COMMENTARY 3

PART 1. ACCOUNTING

Cybersecurity Risks and Accounting Systems 3

SUPPLEMENTAL MATERIALS

How the Accounting Department Can Help with Cybersecurity Risk Management 11

GROUP STUDY MATERIALS

A. Discussion Problems 21

B. Suggested Answers to Discussion Problems 22

PART 2. AUDITING

Group and Compliance Audits 25

SUPPLEMENTAL MATERIALS

ASB Proposals on Group Audits and Compliance Audits 33

GROUP STUDY MATERIALS

A. Discussion Problems 43

B. Suggested Answers to Discussion Problems 44

PART 3. SMALL BUSINESS

Financial Disclosures and Government Assistance 45

SUPPLEMENTAL MATERIALS

Financial Reporting for the Employee Retention Credit 51

GROUP STUDY MATERIALS

A. Discussion Problems 57

B. Suggested Answers to Discussion Problems 58

GLOSSARY OF KEY TERMS 59

CUMULATIVE INDEX 2022 61

CPE QUIZZER 65

Note: Beginning with the March 2023 edition of the Network programs DVDs will no longer be shipped by Thomson Reuters. Videos will be available for download or streaming only. For customers wishing to adopt an online only format sooner, please contact your customer representative.

NOTE: During the COVID-19 crisis, direct person to person contact can be reduced by forwarding this to participants and reminding others that the video is also available online through the CPL player. Additionally, video/discussion/Q&A may be shared via Teams, Zoom, or other conferencing-type software. Participants may submit the quiz for self-study credit, or Group Internet Based credit (similar to a webinar) is now available. Consult the user guide at the end of the newsletter for instructions on how to earn credit in this manner.

Topics for future editions may include:

- Agreed upon Procedure Engagements
- SEC Proposed Climate Change Disclosures
- Accounting and Auditing Cryptocurrency and Other Digital Assets



THOMSON REUTERS®

EXECUTIVE SUMMARY

PART 1. ACCOUNTING

Cybersecurity Risks and Accounting Systems..... 3

Jennifer Louis, CPA discusses cybersecurity risk and how accounting systems can help detect and prevent issues. [Running time: 35:22]

Learning Objectives: Upon completion of this segment, the user should be able to:

- Identify what percentage of cyber leaders feel confident in the cyber resiliency of their organizations
- Identify common cyber threats and detective strategies
- Identify types of attacks and backup methods

PART 2. AUDITING

Group and Compliance Audits..... 25

Jennifer Louis, CPA recent proposed audit guidance on group and compliance audits. [Running time: 34:11]

Learning Objectives: Upon completion of this segment, the user should be able to:

- Identify the effective dates of the proposed guidance
- Define a referred-to auditor, a group auditor, and a component auditor
- Identify who has responsibility to determine sufficient appropriate audit evidence has been obtained
- Identify what addresses aggregation risk in looking at group financial statements

PART 3. SMALL BUSINESS

Financial Disclosures and Government Assistance..... 45

With the enactment of the CARES Act and subsequent pandemic related legislation, government assistance poured out to for-profit entities in ways it never has before. Kurt Oestrieher, CPA, reviews the disclosure guidance released in late 2021 by the FASB for those entities receiving government assistance.

[Running time: 29:48]

Learning Objectives: Upon completion of this segment, the user should be able to:

- Identify the accounting guidance related to government assistance disclosures and the effective dates
- Determine the criteria to qualify for the employee retention credit
- Determine what and how to record/disclose government assistance in the financial statements
- Identify how the majority of 2020 employee retention credits were applied for

ABOUT THE SPEAKERS

Jennifer Louis, CPA, is a CPA and president of Emergent Solutions Group, LLC. She has more than 25 years experience in designing and instructing high-quality training programs. Ms. Louis was previously executive vice president and director of training services at AuditWatch Inc., a premier training and consulting firm serving the auditing profession. She also served as financial/operational audit manager for the AARP, and as an audit manager for Deloitte.

Kurt Oestrieher, CPA is a CPA and partner with the accounting firm of Oestrieher and Company in Alexandria, Louisiana. He is in charge of accounting and auditing services, and is also involved in litigation support and small business consulting engagements. In addition to his client responsibilities, Kurt has served as a discussion leader for numerous accounting and auditing courses. He has served on the AICPA Accounting and Review Services Committee and is currently serving a three-year term on the AICPA Council.

Be sure to include the completed sheet when you request certificates for this event.

Title of Course (Enter full title)	
Date of Class (MM/DD/YYYY)	
Time (Enter time of class)	
Location (Enter location of class)	
Learning Objectives (Refer to executive summary)	
Program Description (Refer to executive summary)	
Instructional delivery method	Group Live
Recommended CPE credit	3.0 Credits
Recommended field of study(ies) (Refer to executive summary)	
Program Level	Update
Prerequisites (Circle One)	<ul style="list-style-type: none">Basic Accounting and Auditing professional experience
	<ul style="list-style-type: none">Basic Tax professional experience
	<ul style="list-style-type: none">Basic Governmental professional experience
Advance preparation	None required
Course registration and, where applicable, attendance requirements ⁽¹⁾	

(1) Insert instructions for your students to register for the class and any other attendance requirements (e.g., bring your laptop, be prepared to work in groups, you will be required to sign in and sign out of the session, etc.)

© 2022 Thomson Reuters/Tax & Accounting. Thomson Reuters, Checkpoint Learning and the Kinesis logo are trademarks of Thomson Reuters and its affiliated companies. All rights reserved. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

—From a Declaration of Principles jointly adopted by a *Committee of the American Bar Association* and *Committee of Publishers and Associations*.

PART 1. ACCOUNTING

Cybersecurity Risks and Accounting Systems

In today's global economy, cybersecurity risks and the ability to prevent attacks on essential systems should be the focus of virtually every CFO. Cybersecurity failure is expected to be a critical threat in the next two years according to the WEF 2022 Global Risks Report, and the importance of the role of finance professionals should not be underestimated.

For a look at threats and prevention techniques related to cybersecurity risk, let's join Jennifer F. Louis, a CPA with Emergent Solutions Group, LLC, and CPE Network's Debi Grove Casey.

Ms. Grove Casey

So today we want to talk a little bit about how the accounting department can help with cyber security risk management. To begin with, why should this topic matter to our audience?

Ms. Louis

Well, certainly cyber security risks are top of mind for any organization. As we think about today's environment, the media is constantly reporting different types of cyber attacks. From stealing customer records to breaches of healthcare records, political incidents, this increase in the frequency and magnitude of these various breaches, attacks, ransomware requests have prompted a response by CEOs CFOs, stakeholders and governing bodies. If we look at a report by the World Economic Forum, they did a 2022 global risk report and they found that only about 19% of cyber leaders felt confident that their organizations are what they called cyber resilient. Ultimately, the threats are outpacing an organization's ability to effectively prevent and respond to them.

Ms. Grove Casey

Well, in general, why would accounting and finance professionals be considered important to the objective of cybersecurity risk management?

Ms. Louis

Well, certainly we have an ability to be analytical, critical thinkers as you're trying to identify threats. We have skills and knowledge that should promote our ability to help prevent and mitigate threats in the end, because of the fact that we, in essence, have innate abilities that might be more attuned with our skillsets that would help an organization try to prevent, but also respond appropriately in the circumstances.

Ms. Grove Casey

Well briefly, what are some of the more common threats that an organization should be aware of?

Ms. Louis

Well, malware is a term that's used for any type of malicious software. That's intended to do a variety of things from stealing credentials to denying service, to actually stealing data or money even. The more common types of malware does include ransomware. So ransomware [is] a particular form of malware designed to block access to a computer system until somebody pays a ransom, but there also are botnets that create networks of interconnected computers that are designed to do a particular bidding as far as a botnet agent from a hacker or a bad actor, malvertising – injecting malicious or malware laden advertisements into some sort of webpage or online advertising network. So part of it can be those whole malware components, but then there's also phishing that we're all probably painfully aware of, where it's trying to lure you into doing something that's ill-advised. It's masquerading as a legitimate or trustworthy source. And it's asking you to execute an attachment or click on a link or do something else with the purpose of stealing sensitive data, information, money, et cetera.

The third bucket that I generally will think about would be application attacks. As we think about application development and how we have complex business applications that are delivered through the web, but also through smartphones and other home devices that might be connected to an internet. If you hear IOT platforms, it's internet of things, and there's a variety of things that can be attached to the internet, like, it could be your music system. It could be the, the controlling your heating and your air conditioning. There's a

variety of things that are connected to internet these days that create a, an opportunity for what we call these application attacks that use as far as the functioning of this internet of things,

Ms. Grove Casey

What are some of the consequences that can result from cybersecurity deficiencies? I'm sure it's not just fines and penalties. I mean, that obviously has a financial impact, but I would think that the consequences go beyond that.

Ms. Louis

Right. As we think about the types of deficiencies that you face, as we talk about cyber deficiencies, there's the more technical deficiencies where I'm exposing things like I didn't have adequate encryption, or I didn't use software protections as we expose sensitive information, right? There's also procedural deficiencies that relate to things like I didn't do my security software updates, or I didn't configure the system appropriately, which also could include user related procedural deficiencies, like poorly chosen passwords. It is, it is the, as we think about the legal consequences with fines and lawsuits, et cetera, that might come out of some sort of cyber incident. But it also is the downtime that you lose as far as the responding to, and trying to fix the issue and the revenue generation opportunities that might be lost, but also the tarnished reputation of your brand. The fact that you may have customer flight, particularly as there was an increasing level of e-commerce, it makes it easier for a customer to just go find somebody else. There are lots of vulnerabilities that can be costly beyond just the immediate effect that you might see with debits and credits in your financial statements.

Ms. Grove Casey

Well, what should be the overall cybersecurity objectives that can influence an entity's ability to meet its other goals?

Ms. Louis

Management should think about cyber risks and think about the risks that could affect an ability to not just have fair presentation of your financial statements, but also to be in compliance with laws and regulations, and to run our operations in an effective and efficient way. As we think about COSO and in internal controls and their integrated framework, they do talk about various objectives as an organization. And we need to ensure

that we're designing and implementing an effectively operating control that enables those multiple objectives to be met. And cyber security objectives are going to have a direct and indirect influence on an organization's ability to achieve those broader objectives. And as we think about cyber security objectives, they typically are broken down to making sure that systems and information are available. That's timely, reliable, continuous access, and use of the systems and information that you're protecting information from unauthorized access and disclosure confidentiality. You're also ensuring that you're preserving the integrity of data, including the destruction or modification of data. And you're guarding your systems, the integrity of processing. You have your information, you have your systems. I also need to guard against the improper use, modification, or destruction of my systems themselves. Those are often thought of as like the primary cybersecurity objectives that you should look at as you're looking at designing controls around those matters.

Ms. Grove Casey

What's the nature of the assets of an entity that need to be most directly identified and managed as it relates to cybersecurity risk?

Ms. Louis

Well, as we think about the assets that you have, it is going to include first of all, what are all your various devices? As we think about portable and mobile end user devices, network devices, this internet of things (IOT) devices, your servers, do I even know what I have, what do I even need to manage? What do I need to inventory and track and monitor, and to think about all of my enterprise assets that are connected to my infrastructure, either physically, but also virtually remotely within the cloud so that I know what I have to monitor and protect within the enterprise. And where do I need the support managing to make sure that unauthorized, unmanaged assets are removed. So, as we think about assets of the entity, part of it is thinking about all these enterprise assets, but then you also have all your software assets that relate to your applications and your operating systems to make sure that only authorized software is installed and executed, and that any unauthorized, unmanaged software is found and is either removed or prevented from being installed or executed. So a lot of times when we're talking about cyber security and they talk about assets, they're really talking about the enterprise assets and the software assets that exist in this virtual environment.

Ms. Grove Casey

Let's talk about some examples of common mitigation techniques to achieve those security objectives.

Ms. Louis

Ultimately, we need preventive controls. So we want to make sure that we have protective controls such as, having confidence in accountability for my users that they're identified, like having a username. We also need to have some means of authenticating that yes, that's you; you have this username and yes, that's you because you have a password or a fingerprint or some other biometric, that's authenticating you. You may have multifactor identification. Where you also have a text code that's sent to another number or email that I have to enter in the code before I can move on in the process. As we think about these preventive controls, it's ultimately making sure that yes, it is this individual that I'm intending to give access to, but I also want to make sure that they're authorized to do what they're asked to do.

So you give various levels of user authority, as you think about different transactions and events that occur. But then we also need to think about encryption, encrypting things. I guess somebody might enter credit card information while that information is either at rest, it's being stored or it's in transit going somewhere else to complete some sort of cycle of a transaction or event, we need to ensure that we have somebody that's administering all of my different enterprise assets and software assets that they're creating and assigning, managing revoking privileges and credentials as needed to the actual enterprise asset, the network, the mobile device, but also the software. And we need to have malware defenses where we do have some sort of applications and controls that will prevent the spread and execution of malicious things that come through when somebody clicked on a link or whatever that might be malware defenses, and then, patch and update management to ensure that we're updating our operating systems, our hardware applications as needed, as these improvements come out to ensure that they're the most up to date things

Ms. Grove Casey

Well, besides the preventative strategies, are there any common detective strategies?

Ms. Louis

It is important that we do have what, what they refer to as event monitoring. You have events that are logged into a file where you could look for unusual patterns of activity and who's logged in what programs did they run, what files were accessed, right? Those are things that we need to ensure is a part of the process I'm going to prevent, order, detect, and correct issues. And there does need to be intrusion detection, prevention systems that are available from an ongoing monitoring type perspective. And you can use some of these systems to make your monitoring more effective, because they can look at all of the available data and look for patterns in the data that might suggest a possible attack or security compromise as a means of thinking about event monitoring event, monitoring, intrusion detection, and prevention systems, but also doing threat monitoring, doing case studies and trying to do things where you're doing a threat intelligence to inform us, intelligence about where we need to maybe develop new controls as we have new and emerging threats and patterns that are existing, that we think about continuous vulnerability management, as we're trying to make sure that we're keeping things as up to date as possible, and then training having security awareness and skills training as well is also going to be critical as you try to make those that work for your organization to be security conscious and know what to do if they are ultimately faced with some sort of threat.

Ms. Grove Casey

Well, I've heard that certificates can be a successful preventive measure. Let's talk about what those are and how they can mitigate that cybersecurity risk.

Ms. Louis

A certificate verifies the indemnity of a sender, and it enables transmission of confidential information that's encrypted to be sent privately, and it enables the receiver to know that information hasn't been tampered with, right, because there might be tamper evidence seals that are not broken. We've looked to see if there are signs of tampering. It can be a significant element of a security system, particularly as it relates to payments or other sensitive information. As we are looking at a variety of applications, including digital signing of documents as well, what happens in a certification is that there is a public half of the certificate that is available, but then there's also a private half of the certificate that is kept secure, and

certificates can be centrally managed to ensure that users have access to the public certificate for someone who wants to send encrypted information, but then we also have the private side. It's almost like it was reading about blockchain, where there's a public key and a private key in a blockchain scenario. It's similar in concept to that. What can happen with these certificates is it can help circumvent man in the middle (MiM) type attacks where you know, ultimately as you look at connections between two parties that, in essence, they think they're communicating with each other directly. When in fact, the attacker is a man in the middle that's controlling the conversation. And these certificates are a means of having tampering evidence that would be created to let you know that there's a risk that this might not be who you think the information was supposed to be coming from.

Ms. Grove Casey

Well, is there value in centralized management of systems when there are a variety of access points?

Ms. Louis

Absolutely. As we think about the variety of access points that come from desktops, laptops, mobile devices and centralized management is a way to make sure that as we're looking at things that might be where we can push security protocols, software updates, patches, right. To the various access points and the more centralized we are with our ability to do that, we know directory of what are all our enterprise assets, what are all these access points? And who are the users ultimately that should be having access to these enterprise assets, which is important, particularly when we talk about the mobility that exists and how sometimes devices can have a risk of being lost or stolen, and that creates unique challenges where a laptop, it might be more important to have whole disk encryption and to have that essential to securing the data on a laptop type project, that's more mobile.

If we have third party mobile devices out there that exists, is it a company-owned device? Is it a privately-owned device? And how are we going to ensure there's security on these mobile devices? And particularly if you might have a bring your own device program and it's an employee-owned device, and, and do they need to submit those devices to companywide management, similar to a laptop, how are we going to ensure that we have that centralized management? So certainly, as we think about the access points, but then also just the

overall configuration of the network, as we think about how can we make it exceedingly difficult to circumvent our configurations that exist, and how we can have firewalls to restrict access to certain things, including restricting access to maybe social media and other things like that that might be outside of what we're willing to manage in a centralized way. Those can be the case as well. And then just in general anti-virus and endpoint products that might exist within all of these different access points.

Ms. Grove Casey

Can you discuss why appropriate data backups are so crucial?

Ms. Louis

Well certainly breaches can sometimes go undetected for a period of time, and it's important to have multiple versions of backups so that we can have something that we can go back to

Ms. Grove Casey

If we need to do a restore

Ms. Louis

Exactly with some backups being stored off site. So if there is a ransomware attack, that is keeping my ability again, to get in my system, I do have backups that are stored off site that wouldn't be a part of that ransom attack. A common method is thinking about, I need three copies of data, two of which are backups on different types of media. And one of those backups being stored off site, the 3, 2, 1 model is something that's commonly applied.

Ms. Grove Casey

Well, how should an organization respond when a threat has been discovered to have occurred?

Ms. Louis

If we know a system's been breached, the first level of analysis should be looking to see what's been compromised, right? What changes were made as you look at doing a system level analysis, then as we think about the databases and the variety of means of where data can be stored, including in cloud environments, it's important to do a storage analysis. And that might mean that I need to think about when I do have service providers and what's their requirements to cooperate

with me, as we think about the external ownership of certain servers that do contain my data. And then I also need to think about my network analysis, what traffic occurred and, as we think about the content of what is coming in and what is going out of my network, so that I can also analyze that appropriately. So there's various levels of things, as we think about the value of responding to a threat that I do need to kind of segregate into these different categories.

Ms. Grove Casey

Do organizations find penetration testing effective in preventing breaches?

Ms. Louis

Oh, absolutely. Finding the weak points in your software, in your network if I find my weaknesses, it's possible for me to fix them before a bad actor can take advantage of that weakness, so there can be where we do penetration testing though. The first thing is to identify all of my enterprise assets, right? All of my network components, which does include smart devices, like my internet of things components, which can be televisions, printers, home computer systems, other points of access that do need to be considered for that penetration test. As we think about doing a review of our security, we do need to think about the design, and the design or architectural weaknesses, particularly in areas of sensitivity like payment information, customer records. We need to think about looking at our coding and verifying and authenticating some things that might be weaknesses in our code, but then also doing security testing. So the design, the implementation and operating effectiveness, and then security testing to look at the resilience around some of our vulnerabilities, as we look at the variety of components.

Ms. Grove Casey

How are financial assets deemed to be vulnerable to cybersecurity risks?

Ms. Louis

Well, obviously, cyber attacks generally have a financial or economic motivation. Yes, they might be trying to actually steal my cash, but finance professionals can also play a critical role in thinking about the financial data and business plans, as well as we think about what might be an asset. It's not just cash investments, it's important to think about the

vulnerabilities that you might have as you think about your accounting and finance structure. That can be the beginning part of, as we look about key financial data assets, software applications, cloud-based solutions, and trying to look at those vulnerabilities. There was a study in July of 2021 by a company called Netskope that said that 68% of malware downloads came from these cloud-based applications. And as a gatekeeper of transactions with outside suppliers, the finance team is the one that would know when we have a third-party risk, because I'm paying somebody to be our outsource provider. So I'm the one that can be aware of where those potential vulnerabilities, need to ultimately be managed because of the fact that a third-party vendor supply chain participant ultimately can find that those relationships create vulnerabilities and finance can ensure an enterprise-wide risk-management process is being reviewed as they can know who are we engaged with in some form of customer-vendor relationship that creates a risk.

Ms. Grove Casey

Well, how can accounting and finance contribute to building a culture that's concerned about cyber security?

Ms. Louis

Well, the number one cause of data breaches is often human error and leadership of the finance team can build a culture, ensuring that the finance professionals abide by standards and use appropriate resources and follow protocols as they're looking to comply with a variety of policies and procedures that exist. And in addition, employees should not be punished for trying to report something suspicious. We need to have an environment that welcomes whistle blowers.

Ms. Grove Casey

Well, how can accounting and finance help communicate the consequences of the cyber attacks?

Ms. Louis

Well, certainly we can communicate as far as a financial effect either currently, or like on future projections that might exist with financial data. But they also though, could beyond just the economic damage talk about the effect of reputational risk that could exist as we lose a customer, or the fact that vendor data is exposed, right? They can also focus on that aspect of things as well as they're trying to

communicate effect. It's the tangible and the intangible effects. And, ultimately, as a cyber attack occurs, it can certainly be magnified if the company attempts to cover it up or fails to report and deal with the issue in a timely way, economic damages can come from financial assets being lost, but it also can come from business interruption, and other things that could be a domino from that.

Ms. Grove Casey

Well, obviously, accounting and finance influences the budgeting process. What factors should be considered to ensure there's adequate budget for cybersecurity risk management?

Ms. Louis

A very important thing, because finance is helping put together the budget and setting spending priorities is to say, cybersecurity spending should be an investment, not a cost. You look at an investment and shifting perceptions about securing operations and to focus on enterprise wide risk management and how cybersecurity threats could affect reporting, but also operations and compliance. And there could be litigation and all that things that could come from it. I think having a broad-based perspective in providing informed advice about how to make the best use of cybersecurity spending, but also allocating it appropriately like challenging to make sure that money's being spent in the right areas, that we're not wasting resources analyzing something where that's not really our biggest threat. And, to not just focus on buying technology because it's flashy and new, like what's going to be the benefits or the outcomes from installing this technology. Finance can ask the questions to make sure that the organization is spending their money and in the right ways at the right time, based on their broader based understanding about what might be the right spending choices for the organization as a whole.

Ms. Grove Casey

Well, are there any other areas that accounting and finance can help manage?

Ms. Louis

Certainly, I think as we think about compliance, that they can take a role in understanding the legal and regulatory mandates associated with cybersecurity risk management, with data protection and other things. But

I also think training, as we think about continuously developing the training, the accounting and finance department on new technologies and related cybersecurity controls, including anything that does exist in a cloud-based type environment and that you would enhance and ensure, that this group of individuals is thought of as an in-house resource to having some level of knowledge and ability to be able to look at things from a big picture point of view.

Ms. Grove Casey

In what ways should finance have an influence over those charged with governance as it relates to the cyber issues?

Ms. Louis

Well, I think it's important that we think about, do we have a cyber risk management committee, right? Is there a group, a task force, that's focused on cybersecurity risk management and is somebody that's more senior on the accounting finance team included in that group? If it is a governance committee that has like a board that actually has a subcommittee on cybersecurity risk management, make sure that a senior finance person is involved in communicating with that subcommittee. Ultimately, while you might even have somebody like a chief information officer who oversees any type of incident response plans, the finance team should be involved as well in working with that chief information officer assign somebody to be a part of the initial response team that would be pulled out if there were some sort of breach. There could be, sometimes they're called computer security incident response teams, computer incident response teams, but they have a function of making sure that I can help get the business back on track as far as possible, support legal and forensic investigations as they're needed to put forth a plan of action to communicate with customers, law enforcement, et cetera, having somebody in finance involved in this team, whoever that might be would be critical.

Ms. Grove Casey

So you mentioned task force. And I remember a couple years ago reading that for boards of directors that cyber security issues was one of the key things that they needed to be addressing. And that it was a key focus of most boards of directors for that particular year. And so anytime that we have risk management involved, the word insurance comes up. And so it would seem that

evaluating the adequacy of cybersecurity insurance would also be important. Do you think that, that's the case?

Ms. Louis

Absolutely. As we think about, the policies I have, do I need a separate policy? Do I need a rider? Particularly for organizations that do have significant customer or client personally identifiable information (PII), if you do process online credit card payments, are you otherwise highly dependent on the internet to connect your business? And so there are things where you need insurance that covers your business' assets, like the loss of damage of my data, my software business interruption from network downtime, cyber extortion, customer notification expenses, reputational damage, like those things would all be underneath the first party insurance aspect. But you also need to think about as well, third party insurance that covers the assets of others. Typically like your customers, if there was a security and privacy breach, like the civil damages that might be associated with them. So those, we want to make sure that we're really thinking about what we need, ourselves, but also thinking about others that also might have some sort of claim against us. What additional rider do we need to have to cover those elements?

Ms. Grove Casey

Well, I know the AICPA recently created a cybersecurity risk management reporting framework. What should accounting and finance professionals know about this framework?

Ms. Louis

Well, certainly that's a framework that was developed to help provide context to designing a system that would meet your needs. And it helps as having certain criteria that are consistently looked at in principle in thinking about these risk management frameworks. And so it's certainly a very useful tool to use for both the entities that are designing the systems, as well as any type of audit or attest provider that you have that might be coming in and giving you some form of assurance about those same systems.

Ms. Grove Casey

Well, are these trends and best practices we discussed any different for small businesses than they are for larger ones?

Ms. Louis

Certainly, it's not. All organizations of nature, size and complexity are vulnerable. As we think about cyber attacks and data breaches. And so it is important for all organizations to look at what's needed and in your particular scenario,

How the Accounting Department Can Help with Cybersecurity Risk Management

by Jennifer F. Louis, CPA

Background

Cybersecurity risks should be top of mind for any organization, as it has become a front-and-center issue in today's global economy. The media is buried with reports of cyberattacks ranging from major customer records thefts, health care records breaches, and political incidents. This increase in frequency and magnitude of cyberattacks, data breaches, and ransomware requests has prompted public sector and private sector responses around the world.

Cybersecurity failure is expected to be one of the critical threats the world will be facing in the next two years, according to the World Economic Forum (WEF) 2022 Global Risks Report. This is because cybersecurity threats are outpacing societies' ability to effectively prevent or respond to them, according to the report. The WEF's Global Security Outlook 2022 found that only 19% of cyber leaders feel confident that their organizations are cyber resilient.

Overview of Role of Finance

Organizations should not underestimate how important the role of finance is in managing cybersecurity risks. Finance professionals can use their knowledge and skills to advance efforts to prevent and mitigate cyberthreats within their companies. Finance professionals, who are analytical and experienced in critical thinking, are invaluable to addressing cyber risk.

There are many ways that finance teams can drive the effort to prevent and mitigate cyber risk. Understanding cybersecurity in today's complex digital world begins with knowing what the most common threats are, who the potential 'bad actors' are, and what can be done to shore up defenses.

Common Threats

There are a variety of threats that organizations have become familiar with.

Malware is the term used for malicious software intended to do any number of things ranging from stealing credentials, other information, or money to the

denial of service. Some of the more typical types of malware include:

- Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.
- Botnets are networks of interconnected computers that are infected with a 'botnet agent' designed to do the attacker's bidding.
- Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and web pages.

Phishing usually is an email designed to lure the reader into doing something ill-advised by masquerading as a trustworthy source or legitimate enterprise. Phishing requests to execute an attachment to the email or click on a link are designed to install malware on the user's computer, generally for the purpose of stealing money. Phishing can also involve more direct requests to provide private information, such as passwords, credit card account details or other sensitive data.

Application attacks are increasingly common as application development is moving more and more to the web. In addition to complex business applications being delivered over the web, our personal mobile phone applications and our home devices connected to the internet via Internet of Things (IoT) platforms that create widespread vulnerabilities. While varied in nature and design, application attacks usually have the same intents and purposes as malware attacks—stealing data from database servers, running attack scripts on other users' computers, stealing user credentials, etc.

Types of Deficiencies & Related Consequences

Cybersecurity deficiencies can be technical or procedural. Technical deficiencies that create exposure to sensitive functionality or information include software defects and the failure to use security protections, such as encryption adequately. Procedural deficiencies can be IT-related, including system

configuration mistakes, or failure to keep up with software security updates. However, many procedural deficiencies are user-related, such as poorly chosen passwords.

Whatever the cause, these vulnerabilities can be costly and result in:

- Downtime—Loss of business production or revenue generation opportunities.
- Tarnished reputation—Company and brand value negatively affected.
- Customer flight—Especially critical with increasing level of e-commerce.
- Legal consequences—Fines, lawsuit costs and settlements can be staggering.
- Industry consequences—Health care records breaches have been extensive.

Cybersecurity Objectives

Management establishes cybersecurity objectives that address cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting and operational objectives). They vary depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, risk appetite and other factors.

Key cybersecurity objectives include:

- Availability—Enabling timely, reliable and continuous access to, and use of, information and systems.
- Confidentiality—Protecting information from unauthorized access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements.
- Integrity of data—Guarding against improper information modification or destruction of information.
- Integrity of processing—Guarding against the improper use, modification, or destruction of systems

Identify The Population of What Needs to Be Managed

Control of Enterprise Assets – Actively manage (i.e., inventory, track, and correct) all enterprise assets (e.g., portable and mobile end-user devices; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Control of Software Assets – Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Common Mitigation Efforts

To achieve security objectives and mitigate these risks, implement security mechanisms to protect information assets, detect malicious activity whenever it occurs and respond effectively to that malicious activity to minimize the impact on the business.

Protective controls include:

- Identification—To have confidence in accountability for users, have identification (e.g., usernames).
- Authentication—Authenticate that identification (e.g., passwords, fingerprints, etc.).
- Multi-factor authentication—Require multi-factor authentication (MFA) for accessing your systems whenever possible.
- Authorization—Ensure the user is authorized to conduct transaction (i.e., verify the user's level of authority for particular type of access or transaction).
- Protect secrets (e.g., encryption of credit card information), whether at rest while being stored and in transit.

- Access control management—Use processes and tools to create, assign, manage, and revoke access credentials and privileges for users, administrator and service accounts for enterprise assets and software.
- Malware defenses—Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
- Patch and update management—Enable automatic updates whenever possible, including replacing unsupported operating systems, applications and hardware.

In addition to protective or preventive strategies, it is also essential that entities employ detection strategies to identify when threats occur. Common detection strategies include:

- Event monitoring—Documentation of events logged into files can be reviewed to look for unusual patterns of activity. All modern computer operating systems keep a ledger of their activity—who logged in? What programs did they run? What files were accessed? What were the failures as well as the successes?
- Intrusion detection and prevention systems—Sophisticated applications are available that enable the ability to perform ongoing monitoring. Security information and event management (SIEM) systems have been developed to make monitoring more effective, analyzing all of the available data and look for specific patterns in the data that might suggest a possible attack or security compromise.
- Threat monitoring—Security community can study the tools and techniques that attackers use to develop ‘threat intelligence’ that can be used to inform the development of new controls.
- User reports—User reports can also help identify unusual activity.
- Continuous vulnerability management—Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise’s infrastructure, to remediate, and minimize, the window of opportunity for attackers.
- Audit log management—Collect, alert, review and retain audit logs of events that could help detect, understand or recover from an attack.

- Security awareness and skills training—Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Certificates as a Preventive Measure

Certificates verify the identity of the sender, enable the transmission of encrypted confidential information privately, and enable the receiver to know whether the information has been tampered with via the use of tamper-evident seals. Certificates can be a significant element of security systems, especially where payments or particularly sensitive information is involved. Certificates are used for all kinds of practical applications, including the transmission of confidential information and the digital signing of documents.

There is a public half and private half of a certificate. It is critical that the private half of the certificate be kept secure and not passed between parties. Certificates can be centrally managed to enable users to access the public certificate for someone to whom they want to send encrypted information. For external use, public certificates are issued by third-party certificate authorities that verify the identification of parties using them.

Certificates are essential for circumventing man-in-the-middle (MitM) attacks. MitM is the term used for attacks in which the attacker independently makes connections with the victims and relays messages between them to create the impression that they are communicating with each other when, in fact, the attacker is controlling the conversation.

Centralized Management of Systems of Various Access Points

Desktops—Modern operating systems are full of security features. Centralized management is an important way to control and orchestrate key security features for desktops. The ability to ‘push’ security protocols, software updates and security update ‘patches’ to remote users enables the scalability of security for large enterprise-level systems. Centralization also provides the ability to maintain a directory of user profiles that enables users to access their information from multiple locations.

Laptops—While many security features are common between desktop and laptop computers, the inherent mobility of laptops, especially the risk of lost or stolen devices, presents some unique challenges. Whole disk encryption, whether a feature of the operating system or an endpoint product, is an essential feature to ensure the security of data on laptop products.

Mobile devices—There are third-party mobile device management (MDM) products to facilitate the centralized management of such devices. Some companies consider it important to have company-owned devices and will implement a configuration profile that will prohibit the download of non-company applications.

Many companies have what are referred to as bring-your-own-device (BYOD) programs. To ensure security for these employee-owned devices, they require employees to submit those devices for company-wide management, similar to laptops. To allow for flexibility in the implementation of security policies, companies can create different configuration profiles for different classes of users for their mobile devices.

Network configuration—Another critical component that companies use to enforce policies across the spectrum of corporate networks, that are exceedingly difficult to circumvent.

Network firewalls—Pre-defined policies about who can access what. It can be used to restrict access to social media or other categories of websites. Access control lists implemented at the network level can provide people with access to sites that may not be allowed to others. The communications team, for example, may be authorized to have access to social media sites for company purposes.

Antivirus and endpoint products—In addition to centralized management of security features, most organizations also commonly use ‘endpoint products’ to augment the features that the operating system provides. Endpoint products are especially valuable in ensuring security in enterprise-level systems that multiple users access from multiple locations with multiple devices. These products can ensure compliance with the organization’s policies and standards in addition to verifying the integrity of application products and detecting viruses, blocking activity if issues are found.

The Importance of Back-Ups

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Since breaches can sometimes go undetected for quite some time, it is important to have multiple versions of backups, with some backups being stored off-site to preclude ransomware attackers from encrypting backup files as well as those that are currently active. One common method for maintaining backup files of data is the 3-2-1 model. This model suggests that you need three copies of your data, two of which are backups on different media, and one being stored off-site.

Responding to Threats

In addition to determining what happened, and how a particular breach might be prevented, forensic analysis is the process of examining what is left behind that might be of value to most properly respond to the threat.

- **System-level analysis**—If we know a system has been breached, the first level of analysis would involve looking at the individual system that was compromised for ‘footprints in the sand’ to determine what changes were made.
- **Storage analysis**—The size of today’s databases and the advent of cloud environments complicate storage analysis greatly. A particular complication of cloud environments with respect to forensic analysis involves the external ownership of the servers containing the data. While a subpoena can be issued to the owner of a hard drive containing data that you want to analyze, often the data that you may be interested in may have been deleted and overwritten.
- **Network analysis**—Collecting and analyzing network data ‘traffic’ provides different perspectives. While network monitoring does not provide information about the content of what is coming and going, it does provide information about who is coming and going.

Penetration Testing

The purpose of doing penetration testing is to find the weak points in your software before adversaries find them. If weaknesses are found, it may be possible to fix

them. Otherwise, it may be possible to put in place a detection mechanism to block an intrusion. The first step for penetration testing is to identify all of the network components. This would include all of the ‘smart’ devices including internet of things (IoT) components, and home computer system computers, printers, televisions and other devices that might serve as points of access for an intrusion.

The following are important elements to consider in a security review:

- **Design review**—This involves looking for design or architectural weaknesses. Particular areas of sensitivity are customer records, intellectual property and payment information.
- **Code review**—This includes looking at key areas of sensitivity such as verification and authentication processes and common areas of programming weakness.
- **Security testing**—While penetration testing involves testing the resilience against some set of known software vulnerabilities, security testing is diving deeply into software to verify that security requirements are being properly performed.

Focus on Vulnerable Financial Assets

Cyberattacks are generally financially or economically motivated. Targets include financial data and business plans. Finance professionals can then play a critical role in securing those assets because of their knowledge of how finances are organized, where the key data is, and what systems are used.

Start with identifying key financial data assets and software applications, such as cloud finance solutions, and their vulnerabilities. For example, a total of 68% of malware downloads came through cloud applications, a July 2021 Netskope study found.

As the gatekeeper of transactions with the organization's outside suppliers, the finance team can offer insights on managing third-party risks. Damage can occur when cybercriminals can access an organization's data through its suppliers, subsidiaries, or merger-and-acquisition partners. A World Economic Forum survey found that almost 40% of respondents had been negatively affected by a third-party vendor/supply chain organization cybersecurity incident.

Finance can ensure that any results of any enterprise-wide risk management process is being reviewed by the C-suite and the board and that relevant levels throughout the organization are contributing to it and being made aware of ongoing cyberthreats.

Involve Finance in Governance

All organizations should have a risk security committee that includes a senior finance person and that sets cybersecurity high on its agenda. The board may also need a cybersecurity risk subcommittee, depending on the organization's size and the depth of knowledge available on the board, with a senior finance person involved.

While an incident response plan might be overseen by the Chief Information Officer (CIO), the finance team should be involved as well. If an organization is hit with a ransomware attack and must go off-line for a few days, knowing what the financial impact might be is key. Involve someone who really understands the finances of the business to contribute to that assessment. Assigning a finance team leader to the initial response team to evaluate possible economic damage from an attack and develop effective responses.

Computer Incident Response Teams (CIRTs), sometimes referred to as Computer Security Incident Response Teams (CSIRTS), serve important functions such as:

- Reducing losses
- Helping the business get back into business as soon as possible
- Supporting legal and forensic investigations, when necessary
- Providing decision support during incident-situational awareness, plan of action, informed decisions
- Facilitating crisis communications with customers, law enforcement, media, etc.

Training of Finance Department Staff

Continuing professional development within the finance department should include training on new technologies and related cybersecurity concerns. Cloud migration has enhanced the data backup and recovery, but also added risk. At the same time, the internet of

things (IoT) offers new ways for businesses to create value. However, the constant connectivity and data sharing also creates new opportunities for information to be compromised. Organizations should consider how the metaverse (including digital economy innovations like cryptocurrencies) will affect cyber risk concerns as technology evolves.

Cybersecurity Insurance

Since coverage for damages related to cybersecurity incidents is not included in most commercial insurance policies, a separate policy (or rider) is required. This is especially true for organizations that have significant customer or client personally identifiable information (PII) and process online credit card payments or are otherwise highly dependent upon the web to conduct their business.

In addition to insurance that covers the losses relating to damage to, or loss of information from, IT systems and networks, policies generally include significant assistance with and management of the incident itself, which can be essential when faced with reputational damage or regulatory enforcement. Cyber risks fall into first-party and third-party risks.

First-party insurance covers your business's assets. This may include:

- Loss or damage to digital assets such as data or software programs
- Business interruption from network downtime
- Cyber extortion where third parties threaten to damage or release data if money is not paid to them
- Customer notification expenses when there is a legal or regulatory requirement to notify them of a security or privacy breach
- Reputational damage arising from a breach of data that results in loss of intellectual property or customers
- Theft of money or digital assets through theft of equipment or electronic theft

Third-party insurance covers the assets of others, typically your customers. This may include:

- Security and privacy breaches, and the investigation, defense costs and civil damages associated with them

- Multi-media liability, to cover investigation, defense costs and civil damages arising from defamation, breach of privacy or negligence in publication in electronic or print media
- Loss of third-party data, including payment of compensation to customers for denial of access, and failure of software or systems

While cybersecurity insurance is an important aspect of an organization's strategy, it should not replace best practices, policies, and controls. In fact, having an effective cybersecurity program in place can reduce premiums.

Cybersecurity Risk Management Reporting Framework

In response to the growing demand for information about the effectiveness of organizational efforts to manage cybersecurity threats, the AICPA has developed a cybersecurity risk management reporting framework. While there are many methods and frameworks for developing cybersecurity risk management programs, this framework is a common language for organizations to communicate about, and report on, these efforts.

This framework is designed to help organizations demonstrate to key stakeholders the extent and effectiveness of their cyber risk readiness efforts. Companies can use it internally to explain, in a consistent manner, all of the policies, procedures and controls it has implemented to address the cybersecurity risks that are critical to their business. It can also be used for reporting to senior management, boards of directors and other stakeholders to facilitate their understanding of the entity's cyber risk management program.

Benchmarks, which management can use in describing their cybersecurity risk management program, are captured in the framework's *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*.

An illustrative cybersecurity risk management report has also been developed to provide an example for how an entity might prepare and present a description of its cybersecurity risk management program.

Attestation engagements may be performed to help with cybersecurity risk management.

Focus on Small Businesses

Another notable trend is that data breaches and cyberattacks involving small- and medium-sized businesses are on the rise and failing to address this risk is no longer an option.

Building a culture of cyber readiness has six essential elements for any size organization:

- Entity: Drive cybersecurity strategy, investment and culture.
- Staff: Develop security awareness and vigilance.

- Systems: Protect critical assets and applications.
- Surroundings: Ensure only those who belong on your digital workplace have access.
- Data: Make backups and avoid loss of info critical operations.
- Crisis response: Limit damage and quicken restoration of normal operations.

Common Threats

- Malware
 - Ransomware
 - Botnets
 - Maladvertising
- Phishing
- Application attacks





Cybersecurity Objectives

- Availability
 - Timely
 - Reliable
 - Continuous
- Accessibility and Confidentiality
- Preserving Data
 - Integrity
- Preserving Systems
 - Modification and destruction

Mitigation Techniques

- Accountability and authentication
 - Username and password
 - Biometric or multifactor ID
 - Authority levels
- Encryption
- Accessibility and credentialing
- Malware defense



Detective Strategies

- Event monitoring
- Intrusion detection
- Prevention systems
- Threat monitoring
- Continuous vulnerability management
- Security awareness and skills training



3-2-1 Backup



Cybersecurity aware culture

- Concerns
 - Data breaches
- Solutions
 - Standards and protocols
 - Whistleblowers



Role of accounting and finance

- Communication
 - Reporting internal and external
- Set spending priority and allocation
- Compliance
 - Data protection, regulatory mandates, and risk management
- Work with governance on prevention and response plans



GROUP STUDY MATERIALS

A. Discussion Problems

1. Discuss common cyber security threats.
2. Discuss some common preventive and detective controls that could be suggested by the accounting or finance department to mitigate cybersecurity risks.
3. Discuss the use of cyber security insurance.

B. Suggested Answers to Discussion Problems

1. There are a variety of threats that organizations have become familiar with.

Malware is the term used for malicious software intended to do any number of things ranging from stealing credentials, other information, or money to the denial of service. Some of the more typical types of malware include:

- Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.
- Botnets are networks of interconnected computers that are infected with a ‘botnet agent’ designed to do the attacker’s bidding.
- Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and web pages.

Phishing usually is an email designed to lure the reader into doing something ill-advised by masquerading as a trustworthy source or legitimate enterprise. Phishing requests to execute an attachment to the email or click on a link are designed to install malware on the user’s computer, generally for the purpose of stealing money. Phishing can also involve more direct requests to provide private information, such as passwords, credit card account details or other sensitive data.

Application attacks are increasingly common as application development is moving more and more to the web. In addition to complex business applications being delivered over the web, our personal mobile phone applications and our home devices connected to the internet via Internet of Things (IoT) platforms that create widespread vulnerabilities. While varied in nature and design, application attacks usually have the same intents and purposes as malware attacks—stealing data from database servers, running attack scripts on other users’ computers, stealing user credentials, etc.

Certificates are essential for circumventing man-in-the-middle (MitM) attacks. MitM is the term used for attacks in which the attacker independently makes

connections with the victims and relays messages between them to create the impression that they are communicating with each other when, in fact, the attacker is controlling the conversation.

2. To achieve security objectives and mitigate these risks, implement security mechanisms to protect information assets, detect malicious activity whenever it occurs and respond effectively to that malicious activity to minimize the impact on the business.

Protective controls include:

- Identification—To have confidence in accountability for users, have identification (e.g., usernames).
- Authentication—Authenticate that identification (e.g., passwords, fingerprints, etc.).
- Multi-factor authentication—Require multi-factor authentication (MFA) for accessing your systems whenever possible.
- Authorization—Ensure the user is authorized to conduct transaction (i.e., verify the user’s level of authority for particular type of access or transaction).
- Protect secrets (e.g., encryption of credit card information), whether at rest while being stored and in transit.
- Access control management—Use processes and tools to create, assign, manage, and revoke access credentials and privileges for users, administrator and service accounts for enterprise assets and software.
- Malware defenses—Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
- Patch and update management—Enable automatic updates whenever possible, including replacing unsupported operating systems, applications and hardware.

In addition to protective or preventive strategies, it is also essential that entities employ detection strategies to identify when threats occur. Common detection strategies include:

- Event monitoring—Documentation of events logged into files can be reviewed to look for unusual patterns of activity. All modern computer operating systems keep a ledger of their activity—who logged in? What programs did they run? What files were accessed? What were the failures as well as the successes?
 - Intrusion detection and prevention systems—Sophisticated applications are available that enable the ability to perform ongoing monitoring. Security information and event management (SIEM) systems have been developed to make monitoring more effective, analyzing all of the available data and look for specific patterns in the data that might suggest a possible attack or security compromise.
 - Threat monitoring—Security community can study the tools and techniques that attackers use to develop ‘threat intelligence’ that can be used to inform the development of new controls.
 - User reports—User reports can also help identify unusual activity.
 - Continuous vulnerability management—Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise’s infrastructure, to remediate, and minimize, the window of opportunity for attackers.
 - Audit log management—Collect, alert, review and retain audit logs of events that could help detect, understand or recover from an attack.
 - Security awareness and skills training—Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
3. Since coverage for damages related to cybersecurity incidents is not included in most commercial insurance policies, a separate policy (or rider) is required. This is especially true for organizations that have significant customer or client personally identifiable information (PII) and

process online credit card payments or are otherwise highly dependent upon the web to conduct their business.

In addition to insurance that covers the losses relating to damage to, or loss of information from, IT systems and networks, policies generally include significant assistance with and management of the incident itself, which can be essential when faced with reputational damage or regulatory enforcement. Cyber risks fall into first-party and third-party risks.

First-party insurance covers your business’s assets. This may include:

- Loss or damage to digital assets such as data or software programs
- Business interruption from network downtime
- Cyber extortion where third parties threaten to damage or release data if money is not paid to them
- Customer notification expenses when there is a legal or regulatory requirement to notify them of a security or privacy breach
- Reputational damage arising from a breach of data that results in loss of intellectual property or customers
- Theft of money or digital assets through theft of equipment or electronic theft

Third-party insurance covers the assets of others, typically your customers. This may include:

- Security and privacy breaches, and the investigation, defense costs and civil damages associated with them
- Multi-media liability, to cover investigation, defense costs and civil damages arising from defamation, breach of privacy or negligence in publication in electronic or print media
- Loss of third-party data, including payment of compensation to customers for denial of access, and failure of software or systems

PART 2. AUDITING

Group and Compliance Audits

In March 2022, the Auditing Standards Board issued proposed guidance on group audits and compliance audits. The overall objective of the changes is to strengthen the approach and performance of group audits and to improve the quality of group audits.

For more on what these changes will mean, let's join Jennifer F. Louis, a CPA with Emergent Solutions Group, LLC, and CPE Network's Debi Grove Casey.

Ms. Grove Casey

So today we want to talk a little bit about some ASB proposals on group audits and compliance audits. To begin with, what was the overall objective of the auditing standards board to supersede guidance related to group audits?

Ms. Louis

Well, the goal was to look at as far as what previously was in SAS 122, that related to Section 600 that was a special consideration section that dealt with audits of group financial statements, including the work of component auditors. And they also are looking at expanding that title, in essence, to include not just component auditors, but audits of referred to auditors, which in essence is one special segment around these component auditors, but really to broaden out at least the reinforcement around when these sections apply. So it could be that I'm going to refer to this auditor in my audit report, but it also applies to just component auditors from a broader perspective or point of view. It's more of a principles-based approach that tries to be more adaptable and scalable as you're dealing with different complexities of group audits. And it also tries to create more subsections in order to allow auditors to better understand the requirements that apply in these different levels of complexities, including how much do I have to interact between the group auditors and the component auditors, and applying better definitions, and looking as well around the requirement for the group auditor to identify significant components, and, what's my responsibility for auditing those significant components. In essence, what you do in this new standard is that the group auditor determines an appropriate approach to obtain sufficient appropriate evidence in a group which may or may not involve audit procedures that are being performed at the component level. So not requiring you to do procedures, but still saying you have to get sufficient and appropriate evidence at the end of the day.

Ms. Grove Casey

Well, when is the proposed SAS intended to be effective?

Ms. Louis

It's intended to be effective for audits of group financial statements for periods ending on or after December 15, 2026. So this means that if we're looking at a calendar year-end organization, it would be for 12/31/2026.

Ms. Grove Casey

Was convergence with international audit standards an element of this project?

Ms. Louis

It was to the degree that the auditing standards board feels it's important to make sure that there's not unnecessary differences as we look at what we're doing here in the U.S. compared to the international auditing standards. It's not feasible to comply with fundamentally different group audit standards, particularly when there are situations where different audit reports will say that you complied with both meaning that between the two I comply with the more stringent rule. Well, you can look to see where there's more stringency around the same basic concepts and principles, but when they're vastly different, that is where it eliminates that ability for things to be feasible. And the international standards of audits actually have already made changes related to group financial statement audits. And the ASB did certainly look at that as a basis in developing its own standard to ensure that there was consistency to the degree that it made sense.

Ms. Grove Casey

Well, let's talk about some examples of shared concerns that existed in both the international and U.S. Standards.

Ms. Louis

Alright, so both groups, as we think about the international standard setting board and the audit standards board here in the U.S. previous to making these changes, did have a concern about needing better clarity about whether this section applies. And then if it does, how and to what degree, they felt as if there was also inadequate consideration by the auditor, as they're making decisions about whether to accept or continue with the group audit engagement, including considerations related to complying with a code of professional conduct, to make sure that ultimately you have the competency and can do the work with due professional care and independence and other concerns, but also thinking about how much should this group engagement team be involved in the risk assessment process. Thinking about things broader on just the group financial statement level to design appropriate responses, to identified risks, but also thinking about the significance of things at the component unit level. It really was a concern that went all the way through engagement, acceptance-continuance decisions, all the way through designing and performing your work. But then also what types of communications do we have between the component auditors and the group engagement team, both during the planning risk assessment phase, as well as the performance and evaluating the results of those procedures.

Ms. Grove Casey

What about convergence with the PCAOB auditing standards? Was that goal also embedded into this project because more standards convergence is great on the implementation side, but it sometimes takes a lot longer on the front end.

Ms. Louis

Absolutely. And, just like they don't want to create any differences that were unnecessary between us and international standards, they also don't want to create any unnecessary differences between what auditors do. If you're auditing a public company versus a non-public company, there is a PCAOB release that they've requested as well, comments about supervising audits that involves somebody outside of your accounting firm. And they, as well though, looked at developing their guidance after the international standards of audit that were released. So that in the end, hopefully all of these different standard setting bodies are really working together. So that ultimately, while you have to

really focus on your specific audience, where there may be something specific that you think is necessary, given that context of the type of audit that you're doing, but also trying to work towards that convergence principle.

Ms. Grove Casey

Well, per this new standard, what is the overall objective of group audits?

Ms. Louis

The goal in the end is to determine, as I think I already mentioned before, did I get sufficient appropriate evidence as I'm forming an opinion on the group. And this is going to apply looking at doing a risk assessment of the group financial statements, and to plan and perform further procedures that are responsive to that risk. But as a part of that, though, you have to be sufficiently and appropriately involved with any work of a component auditor, including communications about the scope and timing of the component auditor's work. How does the result of that component auditor's work fit into my ability to make this opinion at the bigger group level? So, as I look at work that's done, whether you're making reference to the component auditor or not in your audit report, I'm still going to use the work of any other auditor informing my opinion and my conclusions, so that really is the broadest based perspective as we think about that overall objective.

Ms. Grove Casey

Well, what's the overall scope and applicability of the requirements for group audits. Did any relevant terminology get clarified or altered?

Ms. Louis

Well, a group would be a reporting entity where group financial statements are prepared. Now group financial statements then would be financial statements that include financial information of more than one entity or business unit, an entity or a business unit through a consolidation process. So they did clarify that a component, it can be an entity, it can be a business unit, it can be a function or business activity or some combination of those. The goal is, as we think about group financial statements through a consolidation process, I'm bringing together financial information of more than one component. And they also talked about what a consolidation process is as we're looking at the SASs. It's not only the preparation of consolidated

financial statements in accordance with the applicable financial reporting framework, as we typically think about consolidation, but it also is the presentation of combined financial statements and the aggregation of financial information of entities or business units, such as divisions or branches of an organization. So in the end, the consolidation process could include what we typically might think of as consolidation, but it also can be proportionate consolidation. It can be equity method of accounting. It can be combined financial statements. It can just be aggregation of financial information. It's a broader perspective of what consolidation really means as you look at complying things as it relates to this particular SAS.

Ms. Grove Casey

Well, does it matter how a group is organized?

Ms. Louis

It can be organized in a variety of ways. A group may be organized by legal entities like a parent and a subsidiary, joint ventures, investments accounted for by the equity method, but also a group can be organized by divisions or branches or geography or functions or business activities, in essence, there's different forms of organization that could apply. And what they're asking is that the group auditor used professional judgment to determine your components. What is a component as we think about things based on an understanding of the group and its environment.

Ms. Grove Casey

So can the standard be adapted to other circumstances, say when a consolidation process is not involved?

Ms. Louis

Absolutely it might be useful when you're looking at, is somebody else attending my physical inventory count or is somebody else inspecting PP&E for me? Are we performing procedures at a shared service center that might be at a remote location that involves another auditor? So while those circumstances don't involve necessarily a component, it still would be useful by principle to adapt the standard as necessary to the circumstances.

Ms. Grove Casey

Well, does this standard apply to all group audits?

Ms. Louis

It applies to all group audits regardless of their size and regardless of their complexity, but what is important is that they're applied in context to the nature and the circumstances of each group audit. It is more of a principle-based approach that is intended purposely to be adaptable and scalable to lots of different circumstances, because I am going to be focusing on a risk assessment first, as I'm deciding what's necessary for me to do in order to get sufficient and appropriate evidence and separate sections throughout the SAS highlight the fact that we do need to think about these circumstances, particularly though when reference is going to be made to a component auditor in the auditor's report, as we're now talking about, it's a referred to auditor in the auditor's report. So part of that would be, as I said, more of a principle-based approach, a more risk-based approach. That's not presuming anything but to allow for you to make judgements and decisions about what's needed to be done at the component level.

Ms. Grove Casey

Well, is there any other new terminology we should be aware of?

Ms. Louis

I've mentioned a couple times the term referred to auditor, which is a new term. And it's defined as an auditor who performs an audit of financial statements of a component to which the group engagement partner determines that we're going to make reference to this auditor in our report on the group financial statements. A component auditor on the other hand is just part of the engagement team and a component auditor ultimately can be any other individuals who perform procedures on an engagement. It can be staff, it can be a partner. It excludes external specialists and internal auditors who might provide direct assistance. Like they're not deemed to be component auditors. That's separate guidance that you would follow in those circumstances. Being that a specialist has to be somebody that's not in the accounting auditing arena that you might be using for a designated purpose.

Ms. Louis

There's separate considerations about using the work of internal audit using the work of an auditor's specialist, but a component auditor would be potentially anybody else that's performing procedures on an engagement. They have made a point though to say, a referred to

auditor is not a component auditor, a component auditor is part of my engagement team, because I'm not going to separately be referring to them in my audit report, a referred to auditor is distinct from that. They're really not considered to be a part of my engagement team. And so that is really a distinction that they're trying to apply, to provide more clarity around what's my responsibilities in each of those two different situations.

Ms. Grove Casey

Well, let's talk a little bit about the concept of group auditor and how that's defined in this proposal.

Ms. Louis

All right. So a group auditor would be the engagement partner and members of the engagement team other than component auditors. And it's the group that is going to be establishing the overall audit strategy and overall plan for the group financial statements. And they will be directing and supervising the components. They'll be reviewing the work of component auditors. They'll be looking at evidence that they get from the component auditors in order to form a conclusion about the overall group financial statements. So there is also a further determination between what's the group auditor and what's the component auditor. Even though, in the end, they're really all working together with the same goal of getting sufficient and appropriate evidence, ultimately, from the group. So it's necessary to carve out component auditors just because of the fact that it's the group auditor and not the component auditors that are responsible for things that they put as a level of responsibility on the group auditor, such as you are the one that's ultimately issuing the opinion, even though you might be using the work of a component auditor.

Ms. Grove Casey

So I'm just mentally trying to get a picture of how this would occur. It makes me think of like different levels of state government. So you have state, county and, and then, maybe city, or borough in some instances where you have some parts are responsible for this and then, other portions, like the county's responsible for some things, but the city's responsible, too. We might have overlapping layers of responsibility there. And that's kind of what I think of when we talk about group auditor, component auditor, and then other people

Ms. Louis

Right.

Ms. Grove Casey

Does this proposed standard address the confusion that often occurs for group auditors in determining what the minimum requirements are when a component auditor is involved compared to when one is not involved?

Ms. Louis

Right. So here's the key, ultimately, is that it can have a circumstance where a group auditor does not involve a separate distinct component auditor. Sometimes the group auditor is the component auditor, right? As I might be engaged to do audits of different parts of the group. So it does in essence, that's where confusion sometimes came into play and what their goal is, is to make it easier for the group auditor to identify which requirements apply and which do not when I really don't have a separate component auditor.

Ms. Grove Casey

Well, to be clear, the group engagement partner may still refer to another auditor in the report, correct?

Ms. Louis

It is, it's still an option to make reference to another auditor. And that's the referred to auditor that we talked about before. What they do in that circumstance is that the auditor's report will say part of this audit was conducted by this referred to auditor. And we'll talk about the source, right? Ultimately, as we think about, how did that segregating its side and saying really I audited everything else, except for this part that was done by this referred to auditor because they have their own report and opinion that's related to that. And in the end, it is the group engagement partner that has to make a decision about, are we going to assume responsibility for the work of this component auditor. Ultimately I have to be required to be involved in the work of this component auditor as relates to my ability to express an opinion on the financial statements, because the component auditor really is a part of the engagement team, even though they're distinct from the group engagement team and the component engagement team, or do I just not accept responsibility and use the reference to refer to option for the audit, of the component auditor as my other alternative, either I'm bringing them into the engagement team or I'm not.

Ms. Grove Casey

Well, who's responsible for determining that sufficient appropriate audit evidence has been obtained?

Ms. Louis

Well in the end, it's always going to be the engagement partner that has to make that determination as they're looking at the, the results of the work. But they can lose resources though that include component auditors, right? Ultimately components are part of my engagement team. Do the engagement team as a whole, were they competent? Did they get sufficient appropriate evidence, as you look at the procedures that the component auditor did in conjunction with the group. And so we should be looking for these component auditors to provide information, perform audit procedures, help us fulfill the requirements that are needed. And sometimes component auditors may have more experience and more in-depth knowledge about a particular component, a particular law, regulation, or business practice. They may know more than the group auditor, but I'm still going to have to oversee the work of the component auditor, right? That's going to be natural, right? Sometimes that you've got within your team, that the team as a whole has necessary competencies and able to get sufficient inappropriate evidence, but there still needs to be the group engagement team partner that is overall having accountability for quality control and ensuring that they're comfortable with what's being done and a supervisor review type process, which would include two-way communication between the group auditors and the component auditors.

Ms. Grove Casey

Well, are there any special planning considerations for group audits?

Ms. Louis

Well, one of the things though is to consider as we look at special considerations for the overall strategy, which one of them can consider the magnitude of the portion of the financial statements that are going to be audited by somebody else in a referred to auditor situation. So as I'm looking at auditing the group, can I get sufficient and appropriate audit evidence of the group? If the magnitude of what I'm saying, I'm not taking responsibility for is proportionately high, right? You still need to think about, am I comfortable with this situation? And that all has to be based on judgment and a principle-based approach as you're trying to determine whether or not that makes sense.

Ms. Grove Casey

Well, we always have materiality considerations in an audit of any sort. And when you're looking at a group audit, are there any special materiality considerations for that?

Ms. Louis

Well, what's quality quantity thing sometimes, to have, a real quality concern, right? That maybe impacts pervasively across the entire group would be what I was thinking about. And so we do look at accounts, class of transactions, disclosures in group financial statements, they're really disaggregated across these components. And as I look at my procedures, the group auditor does need to determine, right, ultimately, as we're looking at the component materiality, it isn't an amount. Then that's set by the group auditor to make sure that I'm reducing my aggregation risk to an appropriately low level and make sure that, it's important for their purposes of planning and performing audit procedures. So there may be a component performance materiality that is different than the group performance materiality. As we look at the group financial statements as a whole, the sense of having a component performance materiality is to address aggregation risk. And, they were saying your performance materiality should be lower compared to your group performance materiality, because as I think about my materiality and then the lower level that I'm actually using to design my scopes and my samples and my acceptance thresholds for analytics, there does need to be a threshold where the group auditor has to decide, well, what threshold am I comfortable with to fully address the aggregation risk, but this threshold for component performance materiality should not exceed the amount that's regarded to be clearly trivial in the group financial statements itself,

Ms. Grove Casey

Do potential access restrictions impact an ability to perform a group audit?

Ms. Louis

It could impact access to ultimately management or governance of a component where I might have limitations in my ability to get certain information at a component, or to be able to have the two-way conversation with a component auditor. Ultimately, if it's not possible because of these restrictions that exist, then I have to think about the effect of that on, do I need

to issue a disclaimer of an opinion on the group financial statements, if I believe that would be the case and, or should we in an initial engagement, just not even accept the engagement or withdraw from the engagement when I'm able to underneath laws or regulations. So they do want to make sure that particularly when it's restrictions imposed by group management on your ability to have access to the component, then I should really stop and think about my ability pervasively to either to get sufficient and appropriate evidence.

Ms. Grove Casey

Well, one of the things about having a group audit is that, we have increased risk. So let's talk a little bit about where the responsibilities for applying professional skepticism might be enhanced in a group audit.

Ms. Louis

Always we need to keep an open questioning mind right throughout the engagement, and they just want to make sure that we emphasize the importance of the group auditor's evaluation of evidence that is coming from the component auditor to keep an open questioning mind about what does that mean? Right. Does the evidence they're getting, does it confirm, does it contradict what the group engagement team is? You, the group engagement team, management of the entity of the group of the reporting entity itself, what they're trying to assert about their financial statements

Ms. Grove Casey

Well, how are required communications enhanced in a group audit?

Ms. Louis

The required communications are just focusing more on strengthening the importance of two-way communication as you're planning, performing, and evaluating the results of the engagement.

Ms. Grove Casey

Well, are there any unique overall responsibilities for a group engagement partner?

Ms. Louis

That the key, which has always been the case, is that the group engagement partner has overall responsibility for quality control on the group audit. And then

therefore they do have to ensure that they set the right environment of establishing two-way communication and that they're sufficiently involved throughout the engagement, including making sure that they're involved in the quality control of the work of the component auditor. So that's just really something that's been more clarified.

Ms. Grove Casey

Well, a lot of times when we have standards that are implemented, there are like for full year financial statements and then interim financial information changes usually occur the following year. Did anything change related to reviews of interim financial information of components?

Ms. Louis

Yes, so Section 930 deals with interim financial information, which includes a reference to significant components and requires the auditor when they're doing a review of interim financial information to get reports from the component auditors, if any exist, related to the review, and to also think about information that they might need to look at, including any investees or any other types of circumstances. So they had to make some changes in that section because of the fact that they made some other changes as it related to the group audits.

Ms. Grove Casey

Well, does this group audit standard have a relationship to compliance audits? Because I know we talked at the beginning that we were going to be talking about the two proposals, but what kind of relationship do they have?

Ms. Louis

When the context, ultimately, as we think about group financial statements and focusing on aggregation risk and a consolidation process, the concepts are, are difficult to apply in a compliance audit because it's a compliance audit engagement, which usually is different than the audit of the financial statements. So there are going to be some conforming things that are in Section 935, that would say that this AU section related to compliance audits to say that it's not applicable, but there would be some communication around that to be able to let you know, like what from the larger SASs applies to compliance audits and what doesn't.

Ms. Grove Casey

Well, I know we mentioned previously that there was a recently issued proposed standard that was related to compliance audits. Let's talk about that a little bit more.

Ms. Louis

Right. So there, there is a separate proposed standard that deals with the fact that there are certain AU-C sections or portions of these AU-C sections that don't make sense to apply to a compliance audit, because they're not relevant to that environment. They don't contribute to meeting the objectives of a compliance audit or it's a subject matter that's already specifically covered by AU-C section 935, that deals with compliance audits. There is an appendix that exists within this AU-C section that deals with things that aren't applicable to compliance audits. And there was a need to go and update that appendix, not just for making a proposed, as we think about the proposed changes for this new group audit situation, but also because of certain changes that were made recently with SAS 142 about using the work of a specialist and how they needed to update that appendix to really take into account all of the recent changes with the SASs.

Ms. Grove Casey

When is the reordering of the appendix intended to be effective?

Ms. Louis

All right. So the reordering of the appendix to just make it in alignment is effective for fiscal periods ending on or after December 15, 2022, as it relates to audit evidence because that's really what's tied to SAS 142 as well.

Ms. Grove Casey

Well, I think there are some other changes to the appendix that were also made besides the simple reordering. So let's talk a little bit about what the nature of those changes are and when they become effective.

Ms. Louis

There were some inconsistencies that were created as well. It wasn't just moving things around administratively. It was actually having to make some actual changes by like adding some paragraph references that needed to be added to the appendix and certain other editorial revisions that had to be made for

clarity and consistency with AU standards. Those standards, as far as the actual changes, not just reorganizing, those are effective for compliance audits for fiscal periods ending on or after December 15, 2023, which is in more alignment with the SASs that relate to say SAS 145 related to risk assessment, which is one of the things that affected this appendix. So making those changes more in alignment with the effective date of those specific SASs versus simply reordering, which could have the earlier effective date as with SAS 142 on audit evidence.

ASB Proposals on Group Audits and Compliance Audits

by Jennifer F. Louis, CPA

Background-Group Audits

In March 2022, the Auditing Standards Board (ASB) issued a proposed Statement on Auditing Standards entitled *Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors and Audits of Referred-to-Auditors)*.

It supersedes Statement on Auditing Standards (SAS) No. 122, Statements on Auditing Standards: Clarification and Recodification, as amended, section 600, *Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors)*. It also amends a variety of other sections of the SAS, including AU-C Section 935, *Compliance Audits*, AU-C Section 230, *Audit Documentation*, AU-C Section 260, *The Auditor's Communication With Those Charged With Governance*, and more.

The overall objective of the change is to strengthen the auditor's approach to planning and performing a group audit and to improve the quality of group audits. For example:

- Reinforcing that all applicable AU-C sections need to be applied in a group audit engagement.
- Establishing stronger links to other AU-C sections.
- Introduces a principles-based approach that is adaptable to a wide variety of circumstances and scalable for audits of groups of different complexity
- Including subsections to better describe the requirements that apply when component auditors are involved, enhancing interactions between group auditors and component auditors.
- Eliminating a requirement for the group auditor to identify significant components and audit those components. Rather, the group auditor determines an appropriate approach to obtain sufficient appropriate audit evidence to address assessed risks of material misstatement of the group financial statements, which may, and often will, involve audit procedures being performed at the component level.

- Providing better definitions and other enhancements.

The proposed SAS would be effective for audits of group financial statements for periods ending on or after December 15, 2026.

Convergence with IAASB

The ASB feels it is particularly important to converge with International Standard on Auditing (ISA) 600, *Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors) (ISA 600 [Revised])*. For firms that perform engagements in accordance with standards of the International Auditing and Assurance Standard Board (IAASB) and the ASB, complying with fundamentally different group audit standards is not feasible.

ISA 600 (Revised) will be effective for audits of group financial statements for periods beginning on or after December 15, 2023.

In converging with the standards of the IAASB, the ASB uses the corresponding IAASB standard as the base in developing its standard. The ASB has made certain changes to the language of the IAASB standard to use terms or phrases that are more common in the United States and to tailor examples and guidance to the U.S. environment. Additionally, consistent with extant AU-C section 600, the ASB has allowed for making reference to another auditor in the auditor's report on group financial statement, which is not permitted under international standards.

Critical concerns shared between the IAASB and ASB include the following:

- Concerns about the scope and applicability of extant ISA 600, including the need for greater clarity about whether, how, and the extent to which ISA 600 applies in certain circumstances
- Inadequate consideration by the auditor of certain matters that may be relevant when deciding whether to accept or continue a group audit engagement

- Inadequate involvement of the group engagement team in assessing the risks of material misstatement at the group financial statement level and in designing and performing appropriate responses to assessed risks (this has been attributed to the fact that the scope of the work in extant ISA 600 focuses on the identification of components and the determination of their significance, rather than on assessing risk)
- Deficiencies in communication between component auditors and the group engagement team during the planning and performance of the group audit
- Variability in the application of the concepts of component materiality and component performance materiality in a group audit, in particular, in relation to the concept of aggregation risk
- The need for additional guidance on documentation related to:
 - Restrictions on access to people or information, and
 - The nature, timing, and extent of the group engagement team's direction and supervision of component auditors and review of their work.

Convergence with PCAOB

In September 2021, the PCAOB issued Release 2021-005, which proposed amendments to its auditing standards related to the supervision of audits that involve accounting firms and individual accountants outside the accounting firm that issues the audit report (i.e., group audits). In developing its proposed SAS, the ASB considered the PCAOB's proposed amendments and noted the fundamental differences between the structure of the IAASB's and PCAOB's standards related to group audits. ISA 600 (Revised) and the proposed SAS contain all the requirements related to group audits in a single standard (i.e., from acceptance and continuance to concluding and reporting, including how the other relevant AU-C sections should be applied in a group audit). In comparison, the PCAOB has several disaggregated standards that address requirements related to various aspects of a group audit.

Overall Objective of Group Audits

The objectives of the auditor are to do the following:

1. With respect to the acceptance and continuance of the group audit engagement, determine whether sufficient appropriate audit evidence can reasonably be expected to be obtained to provide a basis for forming an opinion on the group financial statements
2. Identify and assess the risks of material misstatement of the group financial statements, whether due to fraud or error, and plan and perform further audit procedures to appropriately respond to those assessed risks
3. Be sufficiently and appropriately involved in the work of component auditors throughout the group audit, including communicating clearly about the scope and timing of their work, and evaluating the results of that work
4. Evaluate whether sufficient appropriate audit evidence has been obtained from the audit procedures performed, including with respect to the work performed by component auditors, or through making reference to the audit of a referred-to auditor in the auditor's report on the group financial statements, as a basis for forming an opinion on the group financial statements

Stronger Links to Other AU-C Sections

The proposed SAS clarifies that all AU-C sections need to be applied in a group audit and establishes stronger links to the other AU-C sections, particularly the proposed *Quality Management* SAS; AU-C section 230, *Audit Documentation*; AU-C section 300; AU-C section 315; and AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*. The requirements and application material in the proposed SAS build on, and are consistent with, the principles and requirements in those AU-C sections.

Clarifying Scope and Applicability

The following terminology is consistent with the extant SAS:

- Component: An entity, business unit, function or business activity, or some combination.
- Group: A reporting entity for which group financial statements are prepared.

This proposed SAS revises the definition of group financial statements as: Financial statements that include the financial information of more than one entity or business unit through a consolidation process.

The term consolidation process as used in this proposed SAS refers not only to the preparation of consolidated financial statements in accordance with the applicable financial reporting framework but also to the presentation of combined financial statements and to the aggregation of the financial information of entities or business units, such as branches or divisions.

The consolidation process includes consolidation, proportionate consolidation, inclusion, or an equity method of accounting; the presentation in combined financial statements of the financial information of entities or business units that are under common control or common management; and the aggregation of the financial information of entities or business units such as branches or divisions.

This proposed SAS, adapted as necessary in the circumstances, may also be useful in an audit of financial statements other than a group audit when the engagement team includes individuals from another firm. For example, this proposed SAS may be useful when involving such an individual to attend a physical inventory count; inspect property, plant, and equipment; or perform audit procedures at a shared service center at a remote location.

A group may be organized in various ways. For example, a group may be organized by legal or other entities, such as a parent and one or more subsidiaries, joint ventures, or investments accounted for by the equity method. Alternatively, the group may be organized by geography, by other economic units (including branches or divisions), or by functions or business activities. In this proposed SAS, these different forms of organization are collectively referred to as entities or business units.

The group auditor uses professional judgment in determining the components at which audit work will be performed. This determination is based on the group auditor's understanding of the group and its environment, and other factors such as the ability to perform audit procedures centrally, the presence of shared service centers, or the existence of common information systems and controls.

Introducing Principles-Based Approach

This proposed SAS applies to all group audits, regardless of size or complexity. However, the requirements of this proposed SAS are intended to be applied in the context of the nature and circumstances of each group audit.

The proposed SAS introduces a principles-based approach that is adaptable to a wide variety of circumstances and scalable for audits of groups of different complexity, for example:

- Focusing on identifying, assessing, and responding to the risks of material misstatement.
- Including separate sections throughout the proposed SAS to highlight the requirements and application material for circumstances when component auditors are involved or when reference is made to the audit of a referred-to auditor in the auditor's report on the group financial statements.
- There is no longer a requirement for the group auditor to identify significant components and audit those components. Rather, the group auditor determines an appropriate approach to obtain sufficient appropriate audit evidence to address assessed risks of material misstatement of the group financial statements, which may, and often will, involve audit procedures being performed at the component level.

New Terminology

The proposed SAS introduces the term referred-to auditor and includes all the paragraphs related to making reference to the audit of a referred-to auditor together in one section.

Referred-to-auditor is defined as: An auditor who performs an audit of the financial statements of a component to which the group engagement partner determines to make reference in the auditor's report on the group financial statements.

A component auditor is part of the engagement team defined as: All partners and staff performing the engagement, and any other individuals who perform procedures on the engagement, excluding an auditor's external specialist and internal auditors who provide direct assistance on an engagement.

A referred-to auditor is not a component auditor, and therefore, is not a part of the engagement team for a group audit. A referred-to auditor in the proposed SAS is equivalent to a component auditor to whom the group auditor makes reference in extant AU-C section 600.

The term group engagement team is being replaced with group auditor. Group auditor is defined as: The group engagement partner and members of the engagement team other than component auditors. The group auditor is responsible for the following:

1. Establishing the overall group audit strategy and group audit plan
2. Directing and supervising component auditors and reviewing their work
3. Evaluating the conclusions drawn from the audit evidence obtained as the basis for forming an opinion on the group financial statements

The definition of group auditor clarifies that component auditors are not included in that designation. For purposes of a group audit, it is necessary to carve out component auditors from the definition of group auditor because the group auditor (and not component auditors) are responsible for all the items in the definition of group auditor.

Component Auditor Involvement

The proposed SAS includes a subsection in each section of the proposed SAS that provides considerations for the group auditor when component auditors are involved and identifies those subsections as such. This provides scalability for circumstances in which the group auditor does not involve component auditors and makes it easier for the group auditor to identify which requirements apply and which do not.

Referred-to-Auditor Requirements

The option for the group engagement partner to make reference has been maintained in the proposed SAS. Reference in the auditor's report on the group financial statements to the fact that part of the audit was conducted by a referred-to auditor communicates the source of audit evidence with respect to those components for which such reference is made.

The group engagement partner is responsible for deciding, individually for each component, to either:

- Assume responsibility for, and thus be required to be involved in, the work of a component auditor, insofar as that work relates to the expression of an opinion on the group financial statements, or
- Not assume responsibility for, and therefore make reference to, the audit of a component auditor in the auditor's report on the group financial statements.

Obtaining Sufficient Appropriate Audit Evidence

The engagement partner must determine that sufficient and appropriate resources to perform the engagement are assigned or made available to the engagement team in a timely manner. In a group audit, such resources may include component auditors, who are a part of the engagement team. Therefore, this proposed SAS requires the group auditor to determine the nature, timing, and extent of involvement of component auditors.

The group auditor may involve component auditors to provide information, or to perform audit work, to fulfill the requirements of this proposed SAS. Component auditors may have greater experience with and a more in-depth knowledge of the components and their environments (e.g., local laws and regulations, business practices, language, and culture) than the group auditor. Therefore, component auditors can be, and often are, involved in all phases of the group audit.

This proposed SAS requires sufficient and appropriate involvement by the group engagement partner or group auditor, as applicable, in the work of component auditors and emphasizes the importance of two-way communication between the group auditor and component auditors. In addition, this proposed SAS explains the matters that the group auditor considers when determining the nature, timing, and extent of the direction and supervision of component auditors and the review of their work.

As the magnitude of the portion of the financial statements that is audited by referred-to auditors increases, it is less likely that the group engagement partner can conclude that sufficient appropriate audit evidence can be obtained.

Planning and Performing

The proposed SAS establishes a framework for planning and performing a group audit engagement, which:

- Emphasizes special considerations for establishing the overall group audit strategy and group audit plan and highlights the importance of involving component auditors throughout all phases of a group audit.
- Focuses the group auditor's attention on identifying, assessing, and responding to the risks of material misstatement of the group financial statements and emphasizes the importance of designing and performing procedures that are appropriate to respond to those assessed risks of material misstatement.

Materiality

In applying AU-C section 320, *Materiality in Planning and Performing an Audit*, and AU-C section 450, *Evaluation of Misstatements Identified During the Audit*, when classes of transactions, account balances, or disclosures in the group financial statements are disaggregated across components, for purposes of planning and performing audit procedures, for those components on which the group auditor or component auditor will perform audit procedures, the group auditor should determine the following:

- Component performance materiality. To address aggregation risk, such amount should be lower than group performance materiality.
- The threshold above which misstatements identified in the component financial information are to be communicated to the group auditor. Such threshold should not exceed the amount regarded as clearly trivial to the group financial statements.

Component performance materiality is defined as: An amount set by the group auditor to reduce aggregation risk to an appropriately low level for purposes of planning and performing audit procedures in relation to a component.

Group performance materiality is defined as: Performance materiality in relation to the group financial statements as a whole, as determined by the group auditor.

Documentation

The proposed SAS enhances the documentation requirements and application material to emphasize the linkage to the requirements in AU-C section 230 and the documentation requirements in other relevant AU-C sections and to clarify what the group auditor may need to document in different situations, including when there are restrictions on access to component auditor audit documentation.

Access Restrictions

The proposed SAS clarifies how to address restrictions on access to people and information in a group audit, including restrictions on access to component management, those charged with governance of the component, component auditors, or information at the components.

If the group engagement partner concludes that:

1. It will not be possible for the group auditor to obtain sufficient appropriate audit evidence due to restrictions imposed by group management; and
2. The possible effect of this limitation will result in a disclaimer of opinion on the group financial statements, the group engagement partner should either:
 - In the case of an initial engagement, not accept the engagement, or, in the case of a recurring engagement, withdraw from the engagement, when withdrawal is possible under applicable law or regulation, or
 - When the entity is required by law or regulation to have an audit, having performed the audit of the group financial statements to the extent possible, disclaim an opinion on the group financial statements.

Professional Skepticism

The engagement team is required to plan and perform the group audit with professional skepticism and to exercise professional judgment. The appropriate maintenance of professional skepticism may be demonstrated through the actions and communications of the engagement team, including emphasizing the importance of each engagement team member maintaining professional skepticism throughout the group audit. Such actions and communications may

include specific steps to mitigate impediments that may impair the appropriate maintenance of professional skepticism.

This proposed SAS emphasizes the importance of professional skepticism, including:

- Determining the direction, supervision, and review of the component auditor's work, and
- Making the group auditor's evaluation of whether sufficient appropriate audit evidence has been obtained (including from the work performed by component auditors or through making reference to the audit of a referred-to auditor in the auditor's report on the group financial statements) to provide a basis for forming an opinion on the group financial statements.

Enhanced Communications

The proposed SAS strengthens communications between the group auditor and component auditors, emphasizing the importance of two-way communications.

The proposed SAS clarifies various aspects of the group auditor's interaction with component auditors, including communicating relevant ethical requirements, determining competence and capabilities of the component auditor, and determining the appropriate nature, timing, and extent of involvement by the group auditor in the work of the component auditor.

Engagement Partner Overall Responsibility

The proposed SAS requires the (group) engagement partner to take overall responsibility for managing and achieving quality on the (group) audit engagement. The addition of this requirement is intended to align the requirements in AU-C section 300 with a different proposed SAS and to improve audit quality. The (group) engagement partner's review of the overall audit strategy and audit plan demonstrates that the (group) engagement partner has overall responsibility for the (group) audit engagement.

In doing so, the group engagement partner should do the following:

- Take responsibility for creating an environment for the group audit engagement that emphasizes the expected behavior of engagement team members.

- Be sufficiently and appropriately involved throughout the group audit engagement, including in the work of component auditors, such that the group engagement partner has the basis for determining whether the significant judgments made, and the conclusions reached, are appropriate given the nature and circumstances of the group audit engagement.

Audit Quality

The proposed SAS clarifies how the requirements of a separate SAS on quality management apply to manage and achieve audit quality in a group audit, including sufficient and appropriate resources to perform the engagement, and the direction and supervision of the engagement team and the review of their work.

Reviews of Interim Financial Information of Components

The proposed SAS deletes paragraph 14b of AU-C section 930, *Interim Financial Information*, which includes a reference to significant components and requires the auditor, when conducting a review of interim financial information, to obtain reports from component auditors, if any, related to reviews performed of the interim financial information of significant components of the reporting entity, including its investees, or inquire of those auditors if reports have not been issued.

This is because the proposed SAS eliminates the concept of "significant components" and no longer includes a requirement for the group auditor to identify and audit significant components.

Equity Method Investments

Consistent with extant AU-C section 600, investments accounted for using the equity method (EMIs) are considered components and therefore are subject to the scope of the proposed SAS. Currently, the proposed SAS includes application material related to EMIs and provides guidance on how the group auditor may use the work of an audit that has already been completed, which sometimes occurs with EMIs.

Relationship to Compliance Audits

AU-C section 935, *Compliance Audits*, addresses the application of GAAS to a compliance audit.

The proposed SAS is written in the context of group financial statements with a focus on a consolidation process and aggregation risk. The concepts therein are difficult to adapt and apply to a compliance audit due to the nature of that engagement, which differs from an audit of financial statements. Therefore, the conforming amendments related to AU-C section 935 indicate that AU-C section 600 is not applicable to a compliance audit.

A proposed new requirement is being added to AU-C section 935 to address situations in which the auditor uses the work of another auditor. This requirement is similar to the requirement in AT-C section 105, *Concepts Common to All Attestation Engagements*, related to using the work of another practitioner, which applies to examinations of compliance that are required by a governmental audit requirement to be performed under the attestation standards.

However, the proposed new requirement in AU-C section 935 uses language that is aligned with U.S. GAAS, particularly language within the proposed group audits SAS and the proposed SAS *Quality Management for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards*.

Overview – Amendment to Compliance Audits

In February 2022, the ASB issued a proposed statement on auditing standards entitled, *Amendment to AU-C Section 935*, which related to compliance audits.

Certain AU-C sections, or portions thereof, are not applicable to a compliance audit because (a) they are not relevant to a compliance audit environment, (b) the procedures and guidance would not contribute to meeting the objectives of a compliance audit, or (c) the subject matter is specifically covered in AU-C section 935.

AU-C sections, or specified requirements thereof, are identified in the appendix to AU-C section 935, “AU-C Sections That Are Not Applicable to Compliance Audits” (the appendix).

Appendix Reordering

The amendments in SAS No. 142 moved what had been paragraph .08 of AU-C section 500A, relating to *using the work of a management’s specialist*, to become

paragraph .27 of AU-C section 501, without any substantive changes to that paragraph. This paragraph was applicable to compliance audits when it was in AU-C section 500A, and that applicability didn’t change when it was relocated. Therefore, the appendix is proposed to be revised to reflect the continued applicability of this paragraph in a compliance audit.

No other paragraph in AU-C section 501 applies to a compliance audit.

The effective date would be for fiscal periods ending on or after December 15, 2022 for the appendix that relates to AU-C section 501, *Audit Evidence—Specific Considerations for Selected Items*.

Inconsistencies in Appendix

There is an inconsistency in extant AU-C section 935 whereby the requirements in AU-C section 315 with respect to significant risks were scoped out of a compliance audit, but the requirements in AU-C section 330 with respect to significant risks were not. This inconsistency has been removed by adding paragraphs .15 and .22 of AU-C section 330 to the appendix.

Paragraph .18 of AU-C section 330 was also added to the appendix, as performing substantive procedures for each relevant assertion of each significant class of transactions, account balance, and disclosure is not applicable in a compliance audit.

Certain other editorial revisions were made for clarity or consistency with other AU-C sections.

All other proposed amendments in this proposed SAS would be effective for compliance audits for fiscal periods ending on or after December 15, 2023. Early implementation is permitted.

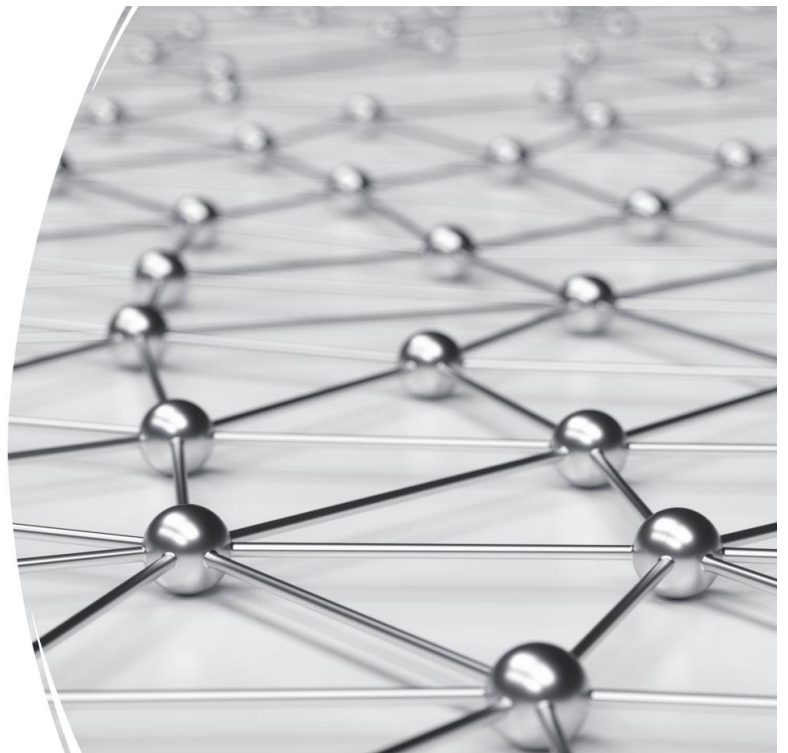
Group audit objective

Obtaining sufficient, appropriate audit evidence in forming an opinion on the group



Component

- Can be an entity
- Can be a business unit
- Can be a function
- Can be a business activity
- Combination of the above



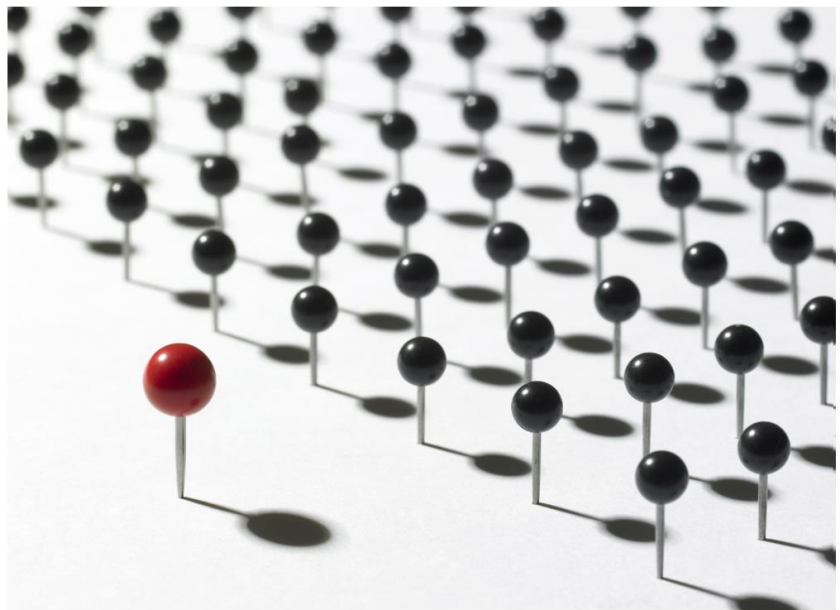
Referred to Auditor

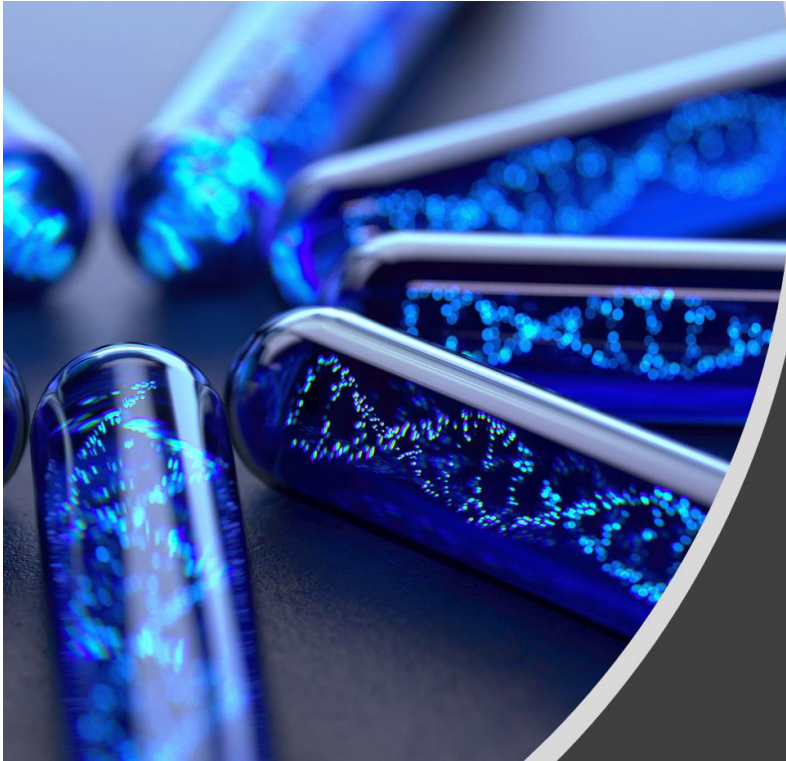
An auditor who performs an audit of financial statements of a component to which the group engagement partner determines reference to this auditor in the report on the group financial statements will be made



Decision?

Group engagement partner decides to refer to an auditor or include them as part of the audit team





Materiality

Component Performance
Materiality set to address
aggregation risk

Compliance audits

- AU-C 935 and the Appendix
 - Appendix reordering becomes effective for periods ending on or after 12.15.2022
 - Appendix conforming changes effective for periods ending on or after 12.15.2023



GROUP STUDY MATERIALS

A. Discussion Problems

1. Discuss critical concerns about group audits between the IAASB and the ASB.
2. Discuss the term group auditor and its responsibilities.
3. Discuss the role of professional skepticism in the proposed SAS.

B. Suggested Answers to Discussion Problems

1. Critical concerns shared between the IAASB and ASB include the following:

- Concerns about the scope and applicability of extant ISA 600, including the need for greater clarity about whether, how, and the extent to which ISA 600 applies in certain circumstances
- Inadequate consideration by the auditor of certain matters that may be relevant when deciding whether to accept or continue a group audit engagement
- Inadequate involvement of the group engagement team in assessing the risks of material misstatement at the group financial statement level and in designing and performing appropriate responses to assessed risks (this has been attributed to the fact that the scope of the work in extant ISA 600 focuses on the identification of components and the determination of their significance, rather than on assessing risk)
- Deficiencies in communication between component auditors and the group engagement team during the planning and performance of the group audit
- Variability in the application of the concepts of component materiality and component performance materiality in a group audit, in particular, in relation to the concept of aggregation risk
- The need for additional guidance on documentation related to:
 - Restrictions on access to people or information, and
 - The nature, timing, and extent of the group engagement team's direction and supervision of component auditors and review of their work.

2. The term group engagement team is being replaced with group auditor. Group auditor is defined as: The group engagement partner and members of the

engagement team other than component auditors. The group auditor is responsible for the following:

- Establishing the overall group audit strategy and group audit plan
- Directing and supervising component auditors and reviewing their work
- Evaluating the conclusions drawn from the audit evidence obtained as the basis for forming an opinion on the group financial statements

The definition of group auditor clarifies that component auditors are not included in that designation. For purposes of a group audit, it is necessary to carve out component auditors from the definition of group auditor because the group auditor (and not component auditors) are responsible for all the items in the definition of group auditor.

3. The engagement team is required to plan and perform the group audit with professional skepticism and to exercise professional judgment. The appropriate maintenance of professional skepticism may be demonstrated through the actions and communications of the engagement team, including emphasizing the importance of each engagement team member maintaining professional skepticism throughout the group audit. Such actions and communications may include specific steps to mitigate impediments that may impair the appropriate maintenance of professional skepticism.

This proposed SAS emphasizes the importance of professional skepticism, including:

- Determining the direction, supervision, and review of the component auditor's work, and
- Making the group auditor's evaluation of whether sufficient appropriate audit evidence has been obtained (including from the work performed by component auditors or through making reference to the audit of a referred-to auditor in the auditor's report on the group financial statements) to provide a basis for forming an opinion on the group financial statements.

PART 3. SMALL BUSINESS

Financial Disclosures and Government Assistance

When the CARES Act passed in March 2020, it started a flurry of legislation that resulted in government assistance to businesses and individuals unprecedented in U.S. history. As a result, the Financial Accounting Standards Board has not previously issued accounting guidance for for-profit entities on the receiving end of this type of funding. There is guidance both internationally and in the not-for-profit literature that entities have used by analogy. However, in November 2021, the FASB did issue guidance on disclosures recipients should be including in the notes to their financial statements.

For more on the financial statement disclosures related to government assistance and uncertainties, let's join Kurt Oestricher, CPA and a partner with Oestricher and Company in Alexandria, Louisiana, and CPE Network's Debi Grove Casey.

Ms. Grove Casey

So today we want to talk a little bit about some recent accounting guidance and the way that it applies to some other things that have been really kind of happening in the news. So last fall, the FASB came out with an ASU on disclosures related to government assistance. Now, sometimes people think about that as only applying to when the government gives you free money or grants but there are other occasions where that may come into play. So let's talk a little bit about that ASU, and then, what kinds of things it does apply to.

Mr. Oestricher

It's the disclosure related to funds received from government assistance that are received by grant or grant analogy. So it's kind of wide open there. And with all the various relief that entities have received through the CARES Act and subsequent acts that provided COVID relief, there are a lot of funds out there and certainly some of the direct payments to medical care providers, nursing homes and especially rural hospitals, I think that absolutely falls under there.

But also, I think things like PPP loans and employee retention credit would also fall under there now. And when you look at the guidance, it doesn't say, oh, and if you received a refundable credit for the employee retention credit, then this fall you have to follow this standard. But there are several things we want to talk about and we want to specifically relate this to the employee retention credit, because even though we thought this was kind of a deal that happened in 2020 and 2021, we're going to talk about so many companies

that are applying for this credit in 2022, they're going back and amending 2020, which is absolutely permitted by the IRS.

Some companies have looked at this, some had looked at it and said no, but now they're getting additional feedback from outsiders that are saying, oh, maybe you really do. So what we need to understand is that if you are receiving some of this government assistance now and the formulas specifically, again talk about the employee retention credit because these are very big numbers that even if you don't believe it necessarily falls under ASU 2021-10, that's the issue that talks about disclosures for entities that receive government assistance.

There's also other disclosures. Like years ago, this would have been considered an extraordinary transaction. So I guess let's walk through what's happening with what the current environment is for the employee retention credit. And then if your entity or your client's entities determine, hey, we're eligible for this, then what are the disclosure requirements related to that for the fiscal year 2022 because this standard was effective for fiscal year beginning after 12/15/21. So we're in that fiscal year now.

Ms. Grove Casey

Well, let's do a little refresher on the employee retention credit because you know, it's been a couple of years, like you said, since it was actually initially released. And not everybody, if you looked at it and evaluated it and said it doesn't apply to my clients, you may not necessarily remember exactly what people qualify for.

Mr. Oestricher

Well, the first thing that happened was when the employee retention credit was provided through the Cares Act, which was the first major legislation that provided assistance to businesses, the government said, OK, you get to choose between the loan and employee retention credit. You don't get both. And then later on in the year as we had a national election, gee, imagine that, they kind of changed their mind and said, Oh, you know what? We'll let you have both. And of course, a lot of rules came out as far as you can't use the same wages for both, PPP loans and the employee retention credit, but if you were eligible, then you can still get it, and then there's guidance that was put out on all of this. Now, I understand these amendments happened in very late 2020, early 2021, and then the IRS guidance comes out.

But imagine you're in public practice like I am at that time. Many companies were still dealing with the health side issue of the pandemic. Depending on where you were located, you may still have had restrictions on business. We were overwhelmed still with helping our clients with. Now we're doing PPP round two, because that came out, so many people said, because this is a look back, we're going to wait and look back later on. We're going to handle PPP round two. We've got a tax season to get through. Where I am in Louisiana, we had hurricanes we were recovering from. So it was one of those things that we kind of pushed back until mid-2021. And, that's really when we started looking at this for many of our clients and for many of them we said, Well, you are eligible. And we followed the guidance and we filed the amended 941s for 2020. So this issue was put to bed for many of our clients in 2021. They may have applied in 2021 but received their funding or the payment for the employee retention credit in 2022. So that would impact your 2022 financial statements. Plus, you've got another angle here where many of my clients that we thought we had this issue put to bed, they have been contacted by third-party companies, and I will try to be civil when I discuss this because there are some very good legitimate third party companies out there that specialize in kind of obscure credits and do a very good job of looking at companies and say, look, if we can recover some credits for you, then we will get a percentage of that. Historically, we've had that for all sorts of different types of tax credits. But my experience with my clients and talking to other CPAs is, many of these companies are also doing this now with the employee retention credit. And in my opinion, they are

not properly interpreting the guidance. They are not telling the whole story to my clients. Like in one example, do you as a school and schools were ordered in the state of Louisiana, hey, sorry you couldn't shut down. And so, that if you look at a strict reading, that's a partial suspension of business operations. And so people go yes, we get the credit. But the very next part, initially it was an IRS Q&A, and now this is actually an IRS notice 2021-20. The next part down says, but if you can accomplish and have substantially the same operations, if you telecommute or telework, then you're not eligible for the credit. Well, every school went to in-house learning.

Remote learning and these private schools had no students pull out. They had the same tuition. They had the same payroll. So I determined that. No, when I talk to my clients about it that, sorry, you don't qualify under this reason. Then the credit companies are going to say, you shouldn't read that part. Just look at the first part. The IRS probably can't audit them. That was one excuse that one of these companies gave. Just risk it. The IRS can't possibly audit all of these. Well, I've got a pretty strong opinion on that. If there is a gray area, then absolutely, take your chances with their gray areas. Every entity out there has a constitutional right that has been upheld by the Supreme Court to legally keep their taxes to a minimum.

And I know this is an employment tax credit versus an income tax credit, but I still think it's the same guideline from the courts. But when the IRS has very specific guidance on your very specific situation, and it said you can't take the credit, I believe that's what we have to follow. So as we go through this, understand that especially for those of you in public practice, you're going to be getting calls. Or if you have not already received calls from your clients to say, look, this company says I get the credit and I'm going to get several hundred thousand dollars, and in one case, one of my clients was literally in the millions of dollars. And so these are going to be significant numbers on your financial statements. So the question is, when to measure them, and what are the disclosure requirements?

So but I think before you even get there, CPAs are in. We typically do this. We have a backbone. We order financial statements, it is in our DNA to be professionally skeptical. And while our clients may not want to hear the truth, the best thing your client can do is to tell them the truth. Now, I would absolutely every

time one of my clients brings this up, I look at this with an open mind. There could be something that I missed. There could be something new that has come out that I wasn't aware of. There could be a different angle. So to revisit the potential for the employee retention credit is something we absolutely should do when our clients ask it. But what we cannot do is just say, Oh, some third party gives, we'll give them responsibility and subordinate our judgment. We cannot do that. If a client asks us our professional opinion, we must give it. If you are in business and industry and you know you shouldn't get it and you've already looked at it, but some third party says, Well, we think you can if you know that is in direct contradiction to the guidance you looked at and you don't believe you're eligible, then I caution you on that.

So I guess that's kind of the first step in this entire discussion, is understand these pressures we're under and revisit the issue. And if you believe your company or your clients deserve it, absolutely apply for it. And then, once you do then we have all these disclosure issues that we have. So we will want to spend some time just revisiting some of the rules here. And then we'll talk about the disclosure requirements.

Ms. Grove Casey

That sounds good. Let's start with looking at the requirements for eligibility and probably you want to start with 2020 because that's the furthest year we can go back and apply for.

Mr. Oestrieher

Right, and the rules are completely different for 2020 and 2021, and they're much more generous. It's easier to qualify in 2021 and it is easier that the amount of the credit is greater in 2021, but for 2020 and again for most people those are the years under question because the law came out in early 2021. So people that were eligible in 2021, they were actually applying for the credit in their timely filed quarterly 941s. Some of them were even getting the advance credit, and so I think most of the issues we have that are happening in 2022 are going back to the 2020 credit, which the first thing you have to look at is, did I meet a gross receipts test or did I meet the government order test?

And under the gross receipts test, for 2020, any one quarter in which your gross receipts were 50% or less than the corresponding quarter in 2019, then you automatically qualify but you have to use the same

method of accounting that you do for tax purposes. There was some question initially when it came out, but again, IRS notice 2021-20 is very clear on that. You have to use the same methodology that you use for your income tax reporting. So that's math, that's very simple. Just look at the gross receipts. And I had like one nonprofit organization came so close, they had a fundraiser at the end of one quarter and if they had had it on that following Monday instead of the Friday, then they would have qualified, but sorry, that cash receipt came in on that day. It was even so close if it was deposited or it was deposited that Friday and it cleared the bank that following Monday because they deposited it after the fundraiser, but even then that would have been an interesting gray area. Well, if you deposited Monday, no, you'd probably still because you have cash on hand.... So look at the gross receipts test first, and I think most of us have done that. Make sure you're using the proper method of accrual versus cash.

Ms. Grove Casey

I have to tell you, this sounds like a spreadsheet, right? So that just sounds like I need to have a spreadsheet for this. And it did they meet this criteria that's one box, do I need to make an X there or not, just to keep track of all the different rules that they have that pertain to this. Because there were a number of rules.

Mr. Oestrieher

Right and then for 2021, the test, you only had to have a 20% reduction. So everything else applies, but fortunately you only had to have a 20% reduction and again you compared back to 2019. Now there was a very odd thing that was included in IRS notice 2021-23; 2021-20 is the base guidance that tells us what we do based on the CARES Act. But when the Recovery Act was passed in late 2020, I think it was actually signed in early 2021 IRS Notice 2021-23 came in and said OK, now that the rules have changed here, the additional guidance or everything in 20 stays the same, but in notice 23 we update. And one of the very unique things that people missed, and I missed that the first time I looked at it, for the first quarter you can use for the first quarter of 2021 you can actually use the fourth quarter of 2020 compared to the fourth quarter of 2019 revenue test.

So you probably already did that revenue test in 2020. Let's say there was a 25% reduction. Well that made you ineligible for the fourth quarter in 20, but you're now eligible for the first quarter of 21. So you

absolutely would like to revisit the gross receipts test. Look at that. I don't want to even call it a safe harbor election.

I'm not sure what to call it, but a gift from the IRS is the best way to call it because it wasn't written into law, that's just how they applied the law. But for every other instance it is just a 20% reduction. Now the next thing that you look at is government orders. If you cannot qualify under the gross receipts test, you look at the government orders and this is where there is let's call it disagreements between entities that have looked at this and a lot of CPAs I've talked to and then these credit recovery companies, we will call them that are saying, oh, wait, now you had a little look at this order out here. It has to be a specific government order. It can't be guidance from the CDC or guidance from some other agency. It has to be a specific order from a governmental agency that's enforceable. So it could be a mayor. I know here in Louisiana, New Orleans had far more restrictive measures than the state, that our governor issued. It could be a county wide order. So it is an enforceable order. And it's not just something we get on the news and say, hey, it's a good idea that you social distance. And I know in Louisiana there had to be a complete or partial suspension of operations so when gyms were ordered closed, when movie theaters were ordered closed, you're done. You qualify because you don't. And by the way, if that happened, you probably met the gross receipts test also, but it's automatic. When it came to restaurants, this is where you had partial suspensions. And this is, again, where it was originally an IRS Q&A, but they were eventually put into the IRS notice 2021-20 where it specifically says, so if you have a restaurant that could only do drive thru, that's considered a partial suspension.

So during the time period that that governmental order was in effect, you were eligible for the employee retention credit. So you need to identify, and I know in Louisiana, when Governor Edwards first issued an order, typically they lasted for 30 days and we actually built a database and we went through to the Louisiana governor website and you can find all these executive orders and we identified each order, and then, they did restrict gyms and we put 100%, 50% so that we had this database and we could point to those orders. And unlike the gross receipts test, which makes you eligible for the employee retention credit for the entire quarter in which you had the downturn and the subsequent quarter, because the quarter when you return, when you now no longer meet the threshold, you still receive the credit for

that quarter. So unlike that in a government order. If it's from date one to date two, when that government order stops, then you're no longer under government order. And in general, in Louisiana and this is what I think most states were like this, but in general, most of these orders stopped being effective in very early 2021, because remember, that's when the vaccine had come out. That's when, quite frankly, our nation had grown weary of the various mandates. And so it went from, hey, we're rescinding the orders now. Now some restaurants and some other people still kept voluntarily saying, OK, we're going to have every other booth closed to maintain social distancing and CDC guidelines that doesn't count as a government order and the IRS Notice is very clear if a company voluntarily continues to comply with the governmental order once it expires, or decides to expand on what a governmental order said, that doesn't count, even if you can establish that, well, maybe my business wasn't forced to shut down, but overall, people were scared to get out. Even that doesn't count. Those things are specifically addressed. So the key on eligibility of the government order is to find a government order that is enforceable in your jurisdiction, beginning date and end date and document that this was a full or partial suspension, and again, with restaurants, it was almost every restaurant in every jurisdiction in the United States. And I know there are some states where they never had these restrictions, but the majority of them did even once you're allowed people to come back into your restaurant. If you could only have 50% occupancy, then that was considered a partial suspension and folks, I know that restaurants were doing more business than they ever did thru the drive through because everyone was getting their personal stimulus checks. I have clients that had record sales but because the government said they can't come inside, they're still eligible. And maybe that's an argument I've heard from people that seems like it's unfair because they were making money and they get the credit and other companies that aren't eligible, they were really suffering and they don't get it. There's never been anything fair about tax law so I get the inherent unfairness of it.

I had some clients that are in the restaurant business that were absolutely shocked when they found out they were eligible. Just to show you the inequities within this credit, there was an entity that owned multiple restaurants in two different states and most of the restaurants were in state A, a few were in state B, but because restaurants in State B were subject to the order,

all the restaurants and all the employees of both states were eligible. Again, makes no sense. You would think it'd just be the payroll in the one, but it is an entitywide issue. So I strongly urge anyone that is revisiting this issue to make sure you're eligible. And remember, you also have to document that even if there was a government order that it impacted you. That's again in IRS notice 2021-20.

And when one of my clients was discussing this with the credit company, I finally said, OK, the credit company are saying these orders, which they weren't orders, it was CDC guidance that they were stretching into an order, there are also some Texas issues there we're looking at that just again didn't qualify, but I said, even so can you please tell me (talking to the owner and the chief operating officer) at what point in 2021 did you say, here's a new order and therefore I have to amend our operations, we have to suspend operations, we cannot provide the services, and what kind of work around when did that happen to you in 2021? And after about a minute of silence, the owner spoke, you know, we never had that issue, and I said so that should tell you everything this company is telling you. There was a government order that affected your operations and you were never affected by a government order. That's clue number one that you should not get this. These are the sort of things there could be a two hour discussion. Just we're not going to get into the dollar amounts and all that, but it's the eligibility that seems to be a question here. So that's going to lead in. And I know what your next question is going to be, if you apply for it, what kind of disclosures and uncertainty. So go ahead. Well, yes, get your thoughts on that there and let's talk about how we disclose this.

Ms. Grove Casey

Yes, so there are I mean, even with the PPP loans, we had uncertainties there. You might remember that we had to disclose because until you got the forgiveness, it wasn't free money. I mean, it was sitting out there and people had some uncertainty related to that. But specifically related to the employee retention credit, did you want to talk about any of the qualifications for the wages or that kind of thing? Because all of that creates some uncertainty that may or may not need to be disclosed.

Mr. Oestrieher

Right. Those are the issues. So when we get into the various dollar amounts, again, just from a time limits, remember, in 2020, it's 50% and there's a maximum for

the entire year, and 2021, it's 70% in each quarter. So you can get up to \$28,000 in 2021, but \$5000 in 2020 so I don't think there will be, I think if people get passed and they can document they meet the revenue threshold or they document that yes, like restaurants in Louisiana or bars in Louisiana there's no doubt. I don't think there's any uncertainties there because if you did the math correctly and you can point to that, there's no uncertainty. It is the more ambiguous orders where people are looking at it, where it's in that gray area where you believe, OK, the IRS hasn't properly addressed that.

I have a unique situation that is not addressed in the IRS guidance and I could see where it could go either way. Then I would think you would have an uncertainty. And again, when you think about the disclosures that have been around at least ten years on tax uncertainties, we always think of it in the realm of income tax uncertainties. And again, this is a payroll tax issue, but remember that disclosures are the minimum disclosures required. And when I look at the spirit of the disclosures on tax uncertainties, I personally don't care whether it's an income tax or an employee retention credit, refundable payroll tax credit, it is still something the whole idea is that the government can send in auditors and claw this money back. That's a tax uncertainty as far as I'm concerned. So any of my clients that have decided hey, this is the route to go, which again, that's management decisions that they can make. Heck, we might have looked at them and said, look, this is a very gray area. It's not addressed. If you want to go with it, go with it. But, we need to be prepared in event of an audit that may not go through them, that's fine. But I think those are areas we need to look at disclosing for tax uncertainties of course, the issue has always been, well, gee, if the IRS looks at these financial statements, it's like you're admitting that you think that they're wrong and it's not.

It's just an uncertainty. We have documented this uncertainty. We know the IRS may look at it and we're going to fight tooth and nail because we believe that we qualify under this government order because the specific issues related to this company were not addressed. And so you file for the credit. And the worst thing that can happen is, those aren't the things that get you thrown in jail or huge fines, but if you remember, the IRS has said that there will be no fines if it's good faith. But if it's not good faith, again, if you feel like you have to write that in the disclosure, then I think you should question whether or not you should have applied for the employee retention credit to begin with.

Ms. Grove Casey

So what kinds of things do we need to have in those disclosures?

Mr. Oestrieher

And then, again, we're looking at three areas of guidance here. Again, first ASU 2021-10, the new one on disclosures about entities that receive government assistance. Those disclose the nature of the assistance, which again, I would state look we applied for the employee retention credit. I would state what year because the rules are different. So I would say what year. If you received the credit in 2021 and have already put it on your quarterly reports and received it, but you believe there are some uncertainties, then I would disclose those uncertainties. Again, a lot of those have not yet been audited. If you went back to 2020, pretty much every credit that was received for 2020 was an amended return.

Now certainly some people for the fourth quarter of 2020 went ahead and applied for the credit when they filed their fourth quarter 941 because they had until January 31st 2021 to file for it, so they did it. But again, the majority of 2020 credits are refunds. So I would disclose that amended returns have been filed because most people understand that that takes a long time to get in.

I would disclose the nature of the order or the gross receipts test, and again, you're not going to find this anywhere in any FASB, anywhere in the accounting standards codification that these are the things, there's just general guidance on the government assistance, general guidance on uncertainties, quite frankly, when you look at this, this would have been considered an extraordinary item, however many years ago until they got rid of extraordinary items. These I would call both unusual and infrequent. Definitely at least maybe it's becoming less frequent now because we found that politicians seem to like it, but it's definitely unusual and maybe at one point it won't, but when it happened, I would classify it as at least one of those. So you have to have disclosures about the nature of the transaction. I would disclose that the funds have been received or if they are booked as receivable and the financial statement where they're recorded.

I would not record these as revenues because these are not a contract with customer. I would disclose these on the face of the financial statements as other income. So

remember, not all of your disclosures are in the footnotes. Some of them are on the face of the financial statement. I would also again recommend, this is just Kurt's recommendation, that if you've not received it but you've applied for it, that it be recorded as a separate line item on your balance sheet, not as an other current asset or other receivable. I would put employee retention credit receivable because these numbers have such a tremendous impact on net income, on your current ratio. So if you've had a credit ratio that's been 2.5:1 and all of a sudden it's 12:1, and certainly for some restaurants, that is the case because they don't carry receivables, their inventory is low, but all of a sudden you're going to get back a check for \$400,000 employee retention credit. So that is just the impact that that this is having on your balance sheet and income statement. And, of course, once you receive it in cash, now it's in cash. So you can do whatever you want to with it. There's no separate disclosure. I do know of one company that it was a government order. It was absolutely within the realm, but he still couldn't believe he got it. He literally has put that money in another account and he said, I'm not touching that money until the audit period is passed, which is fine. But now you've restricted and, again, this is a nonprofit, now you have a kind of a board restriction, if you will. So certainly companies that are doing that because a lot of them just can't believe it. Why is the government giving me this? The PPP loan was fine. I'm happy with that. Why are they giving me this extra money? Well, they did so you can have it. So when you step back and you have all the guidance and you have your disclosure checklist, but still, if a reader of the financial statement doesn't understand that you applied for the employee retention credit and you've either received it or booked it as a receivable and the methodology used for eligibility and the fact that it is subject to audit for a certain period of time and the dollar amount, I believe that those items are disclosed.

Now, the user has sufficient information to make decisions as to, OK, what would be the impact on these financial statements? And to our level, or at least then you start up a discussion with management. So that's what we're recommending to our clients. And again, so many of our clients, this has bled into 2022 because we couldn't get to them until 2022 in the first part of the year. That's when we amended or we amended in 2021 and they received the funds in 2022, so it is just an area that we want to highlight for disclosure issues in 2022.

SUPPLEMENTAL MATERIALS

Financial Reporting for the Employee Retention Credit

by Kurt Oestrieher, CPA

Many entities are applying for the Employee Retention Credit by amending Federal Form 941 for both 2020 and 2021. The appropriate accounting treatment for the recognition of the Employee Retention Credit is not directly addressed in the Accounting Standards Codification, and therefore management will have to use judgement in determining when it is appropriate to accrue the credit and the necessity for making a prior period adjustment. Because of the unique provisions of this credit, and the fact that it was made retroactive if an entity had also received a Paycheck Protection Act loan, there is diversity in practice in accounting for the credit. This course is designed to provide sufficient information so that management can make an informed judgement for both recognition and disclosure issues related to the Employee Retention Credit.

Background of the Employee Retention Credit

Coronavirus Aid, Relief, and Economic Security Act (CARES)

The CARES Act, which was signed into law on March 27, 2020 first introduced the Employee Retention Credit. At the time the CARES Act was enacted, an entity had to decide whether the ERC or the PPP loan would provide more relief as an entity could not apply for both. Most entities would receive a greater benefit from obtaining a PPP loan, therefore the ERC was largely ignored as entities were focusing on PPP loan forgiveness and other business disruptions related to the COVID 19 pandemic.

Taxpayer Certainty and Disaster Relief Act of 2020 (Relief Act)

The Relief Act, which was signed into law on December 27, 2020 amended the CARES Act and allowed an entity to take advantage of both the Employee Retention Credit and PPP Loan Program. The Relief Act also extended the Employee Retention Credit to all four quarters in 2021 (the fourth quarter was later rescinded by subsequent legislation, and provided a more generous benefit for 2021).

Benefits available from the Employee Retention Credit

The Employee Retention Credit is a refundable credit payable against the employer portion of payroll taxes. The credit is obtained by filing a 941 when the credit is

available for an entity, or filing an amended return (941X) when an entity later determines that it is eligible for the credit after filing an original 941. The benefits are different for the ERC depending if the qualifying wages were paid in 2020 or 2021. A summary of the benefits are in the Table below.

	2020	2021
ERC as a percent of wages	50%	70%
Wage limit per employee	\$10,000 annual	\$10,000 per quarter
Max ERC per employee	\$5,000 for year	\$7,000 per quarter

The above benefits are available in 2020 for any eligible wages paid to an employee if an employer has fewer than 500 employees. If the employer has more than 500 employees, wages are only eligible for the ERC if the wages were paid to an employee who was not performing any services.

The information above is general in nature and provides a broad overview of the benefits that are available from the ERC. An entity that is exploring the possibility of filing for the ERC should conduct further research on various nuances of the credit.

Eligibility

There are 2 basic tests that are available to determine if an entity is eligible for the ERC. Either one of the tests may be met in order for an entity to be eligible for the credit.

Gross receipts test

The gross receipts test is not subjective. If an entity experiences a decline in gross receipts of 50% or more in any quarter in 2020 compared to the corresponding quarter in 2019, the entity is eligible for the ERC in that quarter. The entity is also eligible in any subsequent quarter that the gross receipts remain under 50%

compared to the corresponding quarter in 2019. The quarter in which gross receipts rises above 50% compared to 2019 is also an eligible quarter. All wages paid within an eligible quarter are qualifying wages. However, the wages must not have been used for PPP loan forgiveness or any other wage credit.

The gross receipts test for 2021 is only a 20% reduction instead of a 50% reduction. All other rules apply. There is a safe harbor available under IRS Notice 2021-23 that will allow an entity to use Q4 2020 receipts compared to Q4 2019 receipts for the Q1 2021 test.

Full or partial suspension of operations due to a government order

Unlike the gross receipts test, this eligibility criteria may be subjective. In certain circumstances, there is no subjectivity. If an entity operates in a state where the governor issued an order that closed a business or reduced the capacity of a business, the law is clear and the entity is eligible for the ERC for the time period that the order is effective. However, judgement is sometimes needed in order to make a determination if a business is partially suspended. An entity should reference IRS Notices 2021-20 (ERC for 2020) and 2021-23 (ERC for 2021) when determining if it is subject to a government order.

During 2022, many companies that offer tax credit recovery services have been contacting businesses and claiming that they are eligible for the ERC and are missing an opportunity. These tax credit recovery companies are offering to prepare the amended 941 forms and are typically charging a percentage of the ERC.

It is the opinion and experience of the author that most of these credit recovery companies are taking ambitious positions that do not align with the specific guidance in IRS Notices 2021-20 and 2021-23. The author has had conversations with some of these credit recovery companies and the positions they were taking can only be characterized as tax fraud. These companies have cited guidance from the CDC and others that clearly do not rise to the level of a government order. They also ignore specific guidance within IRS Notice 2021-20 that an entity must follow when making a determination if they are subject to a government order. An example of this flawed guidance is a belief that a private school is automatically eligible for the ERC if there was a government order that closed schools (which was very common in most states). IRS Notice 2021-20 clearly states (Q&A 15) that if a government order fully or

partially suspends operations, but an entity can continue with comparable operations by requiring employees to telework, the entity is not eligible for the ERC. Most private schools went to a remote learning environment and were able to continue with comparable operations, therefore, they would not be eligible for the ERC.

Any entity that is relying on dubious claims by these credit recovery companies and file for the ERC will have a different set of criteria when determining if it is proper to accrue the credit and also will need to consider additional disclosures. Those disclosure issues are discussed later in this material.

Authoritative Guidance for Financial Reporting

An entity should first consider the requirements of its applicable financial reporting framework when determining the appropriate timing of recognizing the credit. For purposes of this material, we will assume that an entity is applying United States GAAP.

It is the opinion of the author that the guidance in ASC 606 (Revenue Recognition) is not applicable as the ERC does not meet the criteria of a contract with a customer. The author also does not believe that ASC 740 (Income Taxes) apply as the ERC is a reduction of employment taxes not income taxes.

ASC 710(X) (Expenses-Compensation) is the most likely source to find specific authoritative literature on accounting for tax credits against compensation or payroll taxes related to compensation. ASC 710 is silent on the issue, therefore there is no authoritative guidance that an entity is required to be following in recognizing the ERC in financial statements prepared in accordance with United States GAAP. ASC 105-10-05-3 directs an entity to use a non-authoritative source when authoritative guidance is not available. There are many sources of non-authoritative guidance, and the author believes that the most appropriate source for this transaction is the Statement of Financial Accounting Concepts.

Concepts Statement Number 8, which was issued in December, 2021, discusses the attributes of accrual accounting and related concepts. This statement discusses the matching concept, which has not changed over the years. It is the opinion of the author that the benefits received from the ERC should be used to reduce the related payroll and payroll tax expense during the period that the eligible wages are paid. This treatment aligns with the concept that the entity was

under duress during those periods (either through a reduction of revenue or being subject to a government order), and therefore, the benefits of the ERC should reduce expenses in those periods. Some entities may wish to not “net” the ERC against the related payroll expenses, and instead present the ERC as other income during those periods. The author believes this presentation is not only acceptable, but may be preferred due to the unusual nature of the ERC.

If an entity has already released financial statements for a period, and then files amended 941 returns to claim the ERC in those periods, it is the opinion of the author that the expected proceeds of the ERC be treated as a prior period adjustment. However, if there is uncertainty as to whether or not the IRS will grant the refund, then it may be appropriate to not accrue the credit, and therefore no prior period adjustment would be recorded. If the credit is automatic due to the entity meeting either the gross receipts test or there is a specific government order that applies to the entity, it is unlikely that any uncertainty exists. Management should use judgement in determining whether such an uncertainty exists.

Disclosure Requirements

An entity reporting using United States GAAP is required to include informative disclosures for transactions that are unusual in nature or infrequent in occurrence. Because such a generous employment tax credit has never been authorized by Congress in the past, it appears as though the ERC meets the criteria for infrequent in occurrence. The author suggests a separate disclosure that informs the user of the reasons that the entity qualified for the credit, the time period covered by the credit, the amount of the credit accrued, and the date of the filing of the amended return. If the entity filed for the ERC but has not accrued the ERC due to any uncertainty, the author believes this information should be disclosed.

ASC Topic 832 was recently established with the issuance of Accounting Standards Update 2021-10. This topic requires disclosure of transactions with the government that are similar to a grant. The following disclosures are required under this guidance:

- The nature of the transaction
 - General description of the transaction
 - Form in which the assistance is received (cash)

- The accounting policies used to account for the transactions
- The line items on the balance sheet and income statement that are affected by this transaction

Judgement should be used by management when determining if the ERC should be accounted for using a grant analogy. If management concludes that the ERC is similar to a grant, the disclosures should be included. Many of these disclosures will already be covered if management determines that the ERC is infrequent in occurrence.

If there is a significant uncertainty related to the ERC, management should consider disclosing that uncertainty if the ERC has been recorded as a receivable. If the funds are received, management should consider the need to disclose any uncertainty in its tax position and the number of years that the ERC is open to audit by the IRS.

Summary

The Employee Retention Credit is one of the most generous tax breaks offered by the government. Just as with any tax position, there is nothing wrong with claiming any and all tax credits or deductions available to a taxpayer. However, due to the special nature of the ERC, an entity should be very careful when taking uncertain tax positions and relying on shaky advice from an entity with which they have no established relationship. If an entity determines that it is eligible for the ERC, a proper reporting of the transaction needs to be considered, and appropriate disclosures made.

ERC—Employee Retention Credit



- Allowed both ERC and PPP loan
- Cannot use same wages for both
- Different set of rules for 2020 and 2021 for ERC
 - Amount of credit – higher for 2021
 - Limitation on eligible wages – higher for 2021
 - Eligibility based on revenues – lower for 2021
- **BE VERY WARY OF COMPANIES THAT ARE TELLING YOU THAT YOU QUALIFY FOR THE CREDIT**



Guidance

- IRS Notice 2021-20
 - ERC Eligibility
- IRS Notice 2021-23
- ASU 2021-10
 - Government assistance financial statement disclosures



ERC Eligibility 2020

- Full or partial suspension of the operation of business due to government order
- See IRS Notice 2021-20
- Decline in gross receipts
- Decline of more than 50% in any 2020 quarter compared to 2019
- Continues until the entity has at least 80% in gross receipts compared to 2019 quarter.
- ERC ends in the quarter after gross receipts pass the 80% threshold

ERC Eligibility 2021



Full or partial suspension of the operation of business due to government order

- See IRS Notice 2021-23 Amplifies 2021-20 for the Relief Act
- Decline in gross receipts
- Decline of more than 20% in any 2021 quarter compared to 2019
- If not in business in 2019, an entity may use 2020 as the comparison year

Disclosure—Tax Uncertainty

- IRS--a position taken on a tax return for which the corporation or a related party has recorded a reserve in its audited financial statements
- FASB--recognition of tax balances on financial statements that are not recorded on corporate tax returns, if those returns include uncertain tax positions.



Disclosures

- Nature of the assistance
- Funds received or receivable
- Financial statement placement



GROUP STUDY MATERIALS

A. Discussion Problems

1. Discuss the legislation that provided the government assistance related to the employee retention credit.
2. Discuss the full or partial suspension of operations due to a government order criteria for eligibility for the employee retention credit.
3. Discuss the disclosures required by GAAP related to government assistance.

B. Suggested Answers to Discussion Problems

1. There were 2 pieces of legislation related to the employee retention credit (ERC).

Coronavirus Aid, Relief, and Economic Security Act (CARES)

The CARES Act, which was signed into law on March 27, 2020 first introduced the Employee Retention Credit. At the time the CARES Act was enacted, an entity had to decide whether the ERC or the PPP loan would provide more relief as an entity could not apply for both. Most entities would receive a greater benefit from obtaining a PPP loan, therefore the ERC was largely ignored as entities were focusing on PPP loan forgiveness and other business disruptions related to the COVID 19 pandemic.

Taxpayer Certainty and Disaster Relief Act of 2020 (Relief Act)

The Relief Act, which was signed into law on December 27, 2020 amended the CARES Act and allowed an entity to take advantage of both the Employee Retention Credit and PPP Loan Program. The Relief Act also extended the Employee Retention Credit to all four quarters in 2021 (the fourth quarter was later rescinded by subsequent legislation, and provided a more generous benefit for 2021).

2. Unlike the gross receipts test, the full or partial suspension of operations due to a government order eligibility criteria may be subjective. In certain circumstances, there is no subjectivity. If an entity operates in a state where the governor issued an order that closed a business or reduced the capacity of a business, the law is clear and the entity is eligible for the ERC for the time period that the order is effective. However, judgement is sometimes needed in order to make a determination if a business is partially suspended. An entity should reference IRS Notices 2021-20 (ERC for 2020) and 2021-23 (ERC for 2021) when determining if it is subject to a government order.
3. ASC Topic 832 was recently established with the issuance of Accounting Standards Update 2021-10. This topic requires disclosure of transactions with

the government that are similar to a grant. The following disclosures are required under this guidance:

- The nature of the transaction
 - General description of the transaction
 - Form in which the assistance is received (cash)
- The accounting policies used to account for the transactions
- The line items on the balance sheet and income statement that are affected by this transaction

GLOSSARY OF KEY TERMS

Botnets—networks of interconnected computers that are infected with a ‘botnet agent’ designed to do the attacker’s bidding

Component Auditor—An auditor who performs work on the financial information of a component that will be used as audit evidence for the group audit.

Employee Retention Credit (ERC)— A refundable credit payable against the employer portion of payroll taxes it was initially created as part of the CARES Act legislation and then later amended to include 2021 within its scope

Engagement Team—All partners and staff performing the engagement, and any other individuals who perform procedures on the engagement, excluding an auditor’s external specialist and internal auditors who provide direct assistance on an engagement.

Group Auditor—The group engagement partner and members of the engagement team other than component auditors.

Malware—malicious software intended to do any number of things ranging from stealing credentials, other information, or money to the denial of service

Malvertising—injecting malicious or malware-laden advertisements into legitimate online advertising networks and web pages

Phishing—email designed to lure the reader into doing something ill-advised by masquerading as a trustworthy source or legitimate enterprise

Ransomware—malicious software designed to block access to a computer system until a sum of money is paid

Referred-to-Auditor—An auditor who performs an audit of the financial statements of a component to which the group engagement partner determines to make reference in the auditor’s report on the group financial statements

CUMULATIVE INDEX 2022

BY TOPIC

Topic	Month–Page	Topic	Month–Page
Accounting and Financial Reporting for Personal Financial Statements	May-3	Control Deficiency	Mar-48
Accounting and Review Services Committee	May-45	Control Environment	May-27
Accumulated Rights	Jan-4	Control Reliance Plan	May-28
American Rescue Plan	Jun-23	Control Risk	May-30, Aug-48
Analytical Procedures	Jan-43, May-45	Corporate Social Responsibility Reporting	Jul-21
Annual Service Cost	Jul-6	Creditors	Aug-3
Anticipated Forfeitures	Jan-4	Current Expected Credit Loss	Aug-45, 49
Assertion-Level Control	May-28	Cyber Security Risk Management	Sept-3
Assessing Control Risk	May-25	Cybersecurity Risk Management Reporting Framework	Sept-9
Audit Deficiencies	Aug-25	Cybersecurity Risks	Jan-20, Sept-3
Audit Evidence	Aug-43	Debt Instruments	Aug-45
Audit Planning	Aug-46	Deferred Compensation	Jul-3
Audit Risk	May-25	Deferred Compensation Arrangements	Jul-3, Aug-3
Audit Services	Aug-25	Depreciation	Aug-49
Auditing Accounting Estimates	Aug-43	Digital Fluency	Jan-20
Auditor's Point Estimate	Aug-49	Direct Control	May-28
Benefit/User Service Approach	Jul-6	Economic Benefit Doctrines	Aug-5
Binomial Model	Jun-3	Equity Securities	Aug-7
Black Scholes	Jun-3	Employee Retention Credit	Sept-45
Botnets	Sept-3	Engagement Letters	Feb-25
CARES Act	Jun-23, Sept-45	Entity's Ability to Continue as a Going Concern	Feb-5
Cash Basis	Mar-4	Entity-Level Controls	May-28
Code of Professional Conduct	Mar-21	Environmental	Jul-21
Commercial Organization	Jun-25	Equity-Classified Share-Based Awards	Jun-3
Communication	Mar-56	ESG	Jul-21
Compensation	Aug-3	Estimated Current Values	May-4
Compensated Absences	Jan-3	Exit Value	Feb-11
Compilations	Jan-43, Feb-25	Fair Value	Feb-4
Compliance Audit	Jun-24, Sept-25	Financial Reporting Framework	Mar-8
Component Auditors	Sept-25	First Party Insurance	Sept-9
Computer Security Incident Response Teams ..	Sept-8	FRF for SMEs	Mar-10
Constructive Receipt	Aug-5	GAGAS	Jun-25
Contingencies	Feb-3	Going Concern	Jul-41
Contract Assets	Jun-5	Governance	Mar-56, Jul-21
Contract Liabilities	Jun-5	Government Assistance	Sept-45
Contracts with Customers	Jun-5	Government Auditing Standards	Jun-23, 25
Contractual Basis	Mar-7	Government Orders	Sept-48

Topic	Month–Page	Topic	Month–Page
Grantor Trust	Aug-3	Nursing Homes	Sept-45
Gross Receipts Test	Sept-48	Other Comprehensive Basis of Accounting	Mar-3
Group Audits	Sept-25	Other Comprehensive Income	Aug-7
Impairments	Aug-45, 48	Option Pricing Model	Jun-3
Impairment of a Loan	Feb-5	PCAOB	Aug-25
Income Tax Basis	Jun-47	Peer Reviews	May-25
Independence	Mar-21	Penetration Testing	Sept-7
Indirect Controls	May-28	Pension	Aug-48
Inherent Risk	May-29, Aug-48	Personal Financial Statements	May-3
Internal Control	Aug-47	Phishing	Sept-3
Inquiries	Jan-43, May-45	Plan A	Aug-5
In Relation to Opinion	Jun-26	Predictive Tests	May-50
Internal Control	May-27	Preventive Controls	Sept-5
Internal Control Deficiencies	Mar-47	Primary Recipient	Jun-23
Internal Controls Over Compliance	Jun-28	Professional Ethics Executive Committee	Mar-21
International Financial Reporting Standards	Jul-25	Professional Judgment	May-26
Jury Duty	Jan-5	Program Specific Audit	Jun-25
Key Controls	May-28	Provider Relief Fund	Jun-23
Known Events	Jul-42	Public Company Accounting Oversight Board	Aug-25
Lease Accounting	Jun-7	Qualified Compensation Plan	Jul-3
Lease Standard	Aug-43	Qualitatively	Feb-5
Limited Assurance	Jan-43, May-45, 49	Quantitatively	Feb-5
Liquidation Basis of Accounting	Jul-46	Rabbi Trusts	Jan-3, Jul-3, Aug-3
Loss Contingencies	Feb-4	Ransomware	Sept-3
Lump Sum Payments Under Union Contracts ...	Aug-3	Ratio	May-50
Maladvertising	Sept-3	Reasonable Application of a Reasonable Valuation Method	Jun-3
Malware	Sept-3	Regulatory Basis	Mar-7
Management	Mar-56	Relevant Assertion	May-30
Management's Discussion and Analysis	Jul-25	Remote Auditing	Jan-19
Material Weakness	Mar-48, 56, Aug-47	Revenue Procedure	Aug-5
Medicaid	May-48	Review Engagements	Jan-43, May-45
Medical Care Providers	Sept-45	Reviews	Jan-43
Medicare	May-48	Risk Assessment	May-25
Merger and Acquisition	Aug-25	Risk of Material Misstatement	May-25, Jul-23, Aug-48
Military Service	Jan-5	Risks and Uncertainties Disclosures	Feb-7
Non-Federal Entity	Jun-23	Sabbatical Leave	Jan-6
Non-GAAP Measures	Aug-26	Schedule of Expenditures of Federal Awards ...	Jun-26
Non-Qualified Deferred Compensation Plan	Jul-3	Share-Based Awards	Jun-3
Non-Retirement Post-Employment Benefits	Jan-3, Aug-3		

Topic	Month–Page	Topic	Month–Page
Significant Deficiencies.....	Mar-48, 56, Aug-47	Supply Chain Disruption	Aug-26
Single Audit.....	Jun-23	Sustainability	Jul-21
Sinking Fund Approach.....	Jul-6	Tax Basis.....	Mar-3
Social.....	Jul-21	Third Party Insurance	Sept-9
Special Purpose Frameworks.....	Mar-3	Those Charged with Governance.....	Mar-56
Special Purpose Acquisition Companies	Aug-25	Trading Securities	Aug-7
Split Dollar Life Insurance	Jul-4	Treasury Stock.....	Aug-5
Statement of Changes in Net Worth	May-4	U.S. Department of Health and	
Statement of Financial Condition	May-4	Human Services.....	Jun-23
Stock Appreciation Rights.....	Aug-3	User Authority.....	Sept-5
Stock-Based Compensation	Jan-3, Jul-3, Aug-4	Vesting Rights.....	Jan-4
Stock Compensation.....	Jun-3	Whistle Blowers	Sept-7
Subrecipient.....	Jun-23	Whole Disk Encryption	Sept-6
Subsequent Discovery of Facts.....	Jun-47	Yellow Book	Jun-23
Subsequent Events.....	Jun-47	Yellow Light Disclosure.....	Jul-46
Summary of Significant Accounting Policies	Mar-9	Zoom Fatigue	Jan-23

BY CITATION

Citation	Month–Page	Citation	Month–Page
AR-C 70	Feb-26	AU-C §315.....	May-25
AR-C 80	Feb-25	CECL Model	Feb-10
AR-C 90	Jan-43, May-46	ERISA	Jul-3
AR-C 90.25	Jan-44	FASB 5.....	Mar-49
ASC 205-40.....	Jul-49	FASB ASC 450-20-05-6	Feb-11
ASC 450.....	Feb-3	FASB ASC 710	Aug-3
ASC 606.....	May-46, Jun-5	FASB ASC 710-10.....	Aug-3
ASC 710	Jan-3	FASB Statement 114.....	Feb-5
ASC 718.....	Jun-3	SAS 122	Sept-25
ASC 832.....	Jun-8	SAS 134	Aug-45
ASC 842.....	Jun-7	SAS 142	Sept-31
ASU 2014-15.....	Feb-5	SAS 143	May-30, Aug-43
ASU 2016-13.....	Feb-10	SAS 145	May-25, 29, Sept-31
ASU 2021-07.....	Jun-3	Section 205-30	Jul-47
ASU 2021-08.....	Jun-5	SOP 82-1	May-3
ASU 2021-09.....	Jun-7	SSARS 1	May-45
ASU 2021-10.....	Jun-8, Sep 45	SSARS 25	May-49
AU-C 265	Mar-47	Statement of Position 96-1	Feb-12
AU-C 800	Mar-9	Topic 274	May-3, 4

Citation	Month–Page	Citation	Month–Page
Topic 275	Feb-6	Topic 715	Jan-3, Feb-4
Topic 310	Feb-10	Topic 718	Jan-3, Feb-4
Topic 450	Jan-4, Feb-3	Topic 740	Jan-4, Feb-4, Jul-5
Topic 450-30-25-1	Feb-7	Topic 805	Jun-6
Topic 505	Aug-5	Topic 820	Feb-4, May-5
Topic 610-20	Jun-6	Topic 842	Feb-3
Topic 710	Feb-4, Jul-3	Topic 944	Feb-4
Topic 710-10-25-1	Jul-4	Topic 958	Jun-8
Topic 712	Jan-3, Feb-4		

BY SPEAKER

Speaker	Month	Speaker	Month
Russ Madray	Jan-Feb, May-Aug	Kurt Oestrieher	Jan-Mar, May-Sept
Jennifer Louis	Jan, Mar, May-Sept		

Choose the best response and record your answer in the space provided on the answer sheet.

1. According to Jennifer Louis, a 2022 global risk report from the World Economic Forum found that approximately what percentage of cyber leaders were confident in the cyber resiliency of their organization?
 - A. 10%.
 - B. 20%.
 - C. 50%.
 - D. 90%.

2. According to Jennifer Louis, which of the following is a common threat organizations should be aware of?
 - A. Malware.
 - B. Inadequate encryption.
 - C. Poor password choices.
 - D. Lack of software protection.

3. According to Jennifer Louis, which of the following is a common detective strategy to achieve security objectives?
 - A. Usernames.
 - B. Multifactor authentication.
 - C. Biometrics.
 - D. Event monitoring.

4. According to Jennifer Louis, certificates help circumvent which of the following types of attacks?
 - A. Intrusion.
 - B. Password hacking.
 - C. MiM.
 - D. Phishing.

5. According to Jennifer Louis, which of the following is a common method related to backups?
 - A. 3-2-1 model.
 - B. Clone.
 - C. Full backup.
 - D. Differential backup.

Continued on next page

6. According to Jennifer Louis, when is the proposed SAS on group and compliance audits intended to be effective?
 - A. Audits of group financial statements for periods ending on or after December 15, 2023.
 - B. Audits of group financial statements for periods ending on or after December 15, 2024.
 - C. Audits of group financial statements for periods ending on or after December 15, 2025.
 - D. Audits of group financial statements for periods ending on or after December 15, 2026.
7. According to Jennifer Louis, which of the following is new terminology auditors should be aware of?
 - A. Component auditor.
 - B. Referred-to auditor.
 - C. Group financial statements.
 - D. Combined financial statements.
8. According to Jennifer Louis, who is responsible for determining that sufficient, appropriate audit evidence has been obtained?
 - A. An external specialist.
 - B. The component auditor.
 - C. The engagement partner.
 - D. Management.
9. According to Jennifer Louis, which of the following is meant to address aggregation risk in looking at group financial statements as a whole?
 - A. Component performance materiality.
 - B. Group performance materiality.
 - C. Group procedure materiality.
 - D. Portion performance materiality.
10. According to Jennifer Louis, when is the reordering of the appendix related to compliance audits effective with regard to audit evidence?
 - A. For fiscal periods ending on or after December 15, 2022.
 - B. For fiscal periods ending on or after December 15, 2023.
 - C. For fiscal periods ending on or after December 15, 2024.
 - D. For fiscal periods ending on or after December 15, 2026.
11. According to Kurt Oestricher, ASU 2021-10 related to disclosures became effective for which of the following?
 - A. Fiscal years beginning after 12/15/2020.
 - B. Fiscal years beginning after 12/15/2021.
 - C. Fiscal years beginning after 12/15/2022.
 - D. Fiscal years beginning after 12/15/2023.

Continued on next page

12. According to Kurt Oestrieher, which of the following were means by which an entity could qualify for the employee retention credit?
- A. Gross receipts and CDC guidelines.
 - B. Government order and employee loss.
 - C. Gross receipts or government order.
 - D. Government order and inventory obsolescence.
13. According to Kurt Oestrieher, which of the following should **not** be included in the disclosure related to the receipt of government assistance?
- A. The nature of the assistance.
 - B. The year impacted.
 - C. Anticipated plans for the money received.
 - D. When the monies were received.
14. According to Kurt Oestrieher, the majority of 2020 employee retention credits received were which of the following?
- A. Advanced credits.
 - B. Filed with the Form 941.
 - C. Due to an amended return.
 - D. Not applied for.
15. According to Kurt Oestrieher, funds received as a result of the employee retention credit or other government assistance should be recorded as which of the following?
- A. Revenues.
 - B. Other income.
 - C. A contra account against payroll taxes.
 - D. A direct adjustment to equity.

Subscriber Survey Evaluation Form

Please take a few minutes to complete this survey related to **CPE Network® A&A Report** and return with your quizzer or group attendance sheet to 2395 Midway Road, Carrollton, Texas 75006. All responses will be kept confidential. Comments in addition to the answers to these questions are also welcome. Please send comments to **CPLgrading@thomsonreuters.com**.

How would you rate the topics covered in the September 2022 **CPE Network® A&A Report**? Rate each topic on a scale of 1–5 (5=highest):

	Topic Relevance	Topic Content/ Coverage	Topic Timeliness	Video Quality	Audio Quality	Written Material
Cybersecurity Risks and Accounting Systems						
Group and Compliance Audits						
Financial Disclosures and Government Assistance						

Which segments of the September 2022 issue of **CPE Network® A&A Report** did you like the most, and why?

Which segments of the September 2022 issue of **CPE Network® A&A Report** did you like the least, and why?

What would you like to see included or changed in future issues of **CPE Network® A&A Report**?

How would you rate the effectiveness of the speakers in the September 2022 **CPE Network® A&A Report**? Rate each speaker on a scale of 1–5 (5 highest):

	Overall	Knowledge of Topic	Presentation Skills
Jennifer Louis	_____	_____	_____
Kurt Oestrieher	_____	_____	_____

Which of the following methods would you use for viewing CPE Network® A&A Report? DVD ☐ Streaming ☐ Both ☐

Are you using **CPE Network® A&A Report** for: CPE Credit ☐ Information ☐ Both ☐

Were the stated learning objectives met? Yes ☐ No ☐ _____

If applicable, were prerequisite requirements appropriate? Yes ☐ No ☐ _____

Were program materials accurate? Yes ☐ No ☐ _____

Were program materials relevant and contribute to the achievement of the learning objectives? Yes ☐ No ☐

Were the time allocations for the program appropriate? Yes ☐ No ☐ _____

Were the supplemental reading materials satisfactory? Yes ☐ No ☐ _____

Were the discussion questions and answers satisfactory? Yes ☐ No ☐ _____

Specific Comments: _____

Name/Company _____

Address _____

City/State/Zip _____

Email _____

Once Again, Thank You...

Your Input Can Have a Direct Influence on Future Issues!

CPE Network®

Firm/Company Name: _____

Account #:

Location:

Program Title: _____ Date: _____

[illegible]

I certify that the above individuals viewed and were participants in the group discussion with this issue/segment of the CPE Network® newsletter, and earned the number of hours shown.

Instructor Name: _____

Date: _____

E-mail address:

License State and Number:

CPE Network/Webinar Delivery Tracking Report

Course Title	
Course Date:	
Start Time:	
End Time:	
Moderator Name, Credentials, and Signature Attestation of Attendance:	
Delivery Method:	Group Internet Based
Total CPE Credit:	3.0
Instructions:	During the webinar, the moderator must verify student presence a minimum of <u>3 times per CPE hour</u> . This is achieved via polling questions. Sponsors must have a report which documents the responses from each student. The timing of the polling questions should be random and not made known to students prior to delivery of the course. Record the polling question responses below. Refer to the CPL Network User Guide for more instructions. Partial credit will not be issued for students who do not respond to at least 3 polling questions per CPE hour.
Brief Description of Method of Polling	Example: Zoom: During this webinar, moderator asked students to raise their hands 3 times per CPE hour. The instructor then noted the hands that were raised in the columns below.

[illegible]

CHECKPOINT LEARNING NETWORK

CPE NETWORK®

USER GUIDE

REVISED March 11, 2022

Welcome to CPE Network!

CPE Network programs enable you to deliver training programs to those in your firm in a manageable way. You can choose how you want to deliver the training in a way that suits your firm's needs: in the classroom, virtual, or self-study. You must review and understand the requirements of each of these delivery methods before conducting your training to ensure you meet (and document) all the requirements.

This User Guide has the following sections:

- **“Group Live” Format:** The instructor and all the participants are gathered into a common area, such as a conference room or training room at a location of your choice.
- **“Group Internet Based” Format:** Deliver your training over the internet via Zoom, Teams, Webex, or other application that allows the instructor to present materials that all the participants can view at the same time.
- **“Self-Study” Format:** Each participant can take the self-study version of the CPE Network program on their own computers at a time and place of their convenience. No instructor is required for self-study.
- **Transitioning From DVDs:** For groups playing the video from the online platform, we suggest downloading the video from the Checkpoint Learning player to the desktop before projecting.
- **What Does It Mean to Be a CPE Sponsor?:** Should you decide to vary from any of the requirements in the 3 methods noted above (for example, provide less than 3 full CPE credits, alter subject areas, offer hybrid or variations to the methods described above), Checkpoint Learning Network will not be the sponsor and will not issue certificates. In this scenario, your firm will become the sponsor and must issue its own certificates of completion. This section outlines the sponsor's responsibilities that you must adhere to if you choose not to follow the requirements for the delivery methods.
- **Getting Help:** Refer to this section to get your questions answered.

IMPORTANT: This User Guide outlines in detail what is required for each of the 3 formats above. Additionally, because you will be delivering the training within your firm, you should review the Sponsor Responsibilities section as well. To get certificates of completion for your participants following your training, you must submit all the required documentation. (This is noted at the end of each section.) Checkpoint Learning Network will review your training documentation for completeness and adherence to all requirements. If all your materials are received and complete, certificates of completion will be issued for the participants attending your training. Failure to submit the required completed documentation will result in delays and/or denial of certificates.

IMPORTANT: If you vary from the instructions noted above, your firm will become the sponsor of the training event and you will have to create your own certificates of completions for your participants. In this case, you do not need to submit any documentation back to Thomson Reuters.

If you have any questions on this documentation or requirements, refer to the “Getting Help” section at the end of this User Guide **BEFORE** you conduct your training.

**We are happy that you chose CPE Network for your training solutions.
Thank you for your business and HAPPY LEARNING!**

Copyrighted Materials

CPE Network program materials are copyrighted and may not be reproduced in another document or manuscript in any form without the permission of the publisher. As a subscriber of the **CPE Network Series**, you may reproduce the necessary number of participant manuals needed to conduct your group study session.

“Group Live” Format

CPE Credit

All CPE Network products are developed and intended to be delivered as 3 CPE credits. You should allocate sufficient time in your delivery so that there is no less than 2.5 clock hours:

50 minutes per CPE credit TIMES 3 credits = 150 minutes = 2.5 clock hours

If you wish to have a break during your training session, you should increase the length of the training beyond 2.5 hours as necessary. For example, you may wish to schedule your training from 9 AM to 12 PM and provide a ½ hour break from 10:15 to 10:45.

***Effective November 1, 2018:** Checkpoint Learning CPE Network products ‘group live’ sessions must be delivered as 3 CPE credits and accredited to the field(s) of study as designated by Checkpoint Learning Network. Checkpoint Learning Network will not issue certificates for “group live” deliveries of less than 3 CPE credits (unless the course was delivered as 3 credits and there are partial credit exceptions (such as late arrivals and early departures). Therefore, if you decide to deliver the “group live” session with less than 3 CPE credits, your firm will be the sponsor as Checkpoint Learning Network will not issue certificates to your participants.

Advertising / Promotional Page

Create a promotion page (use the template after the executive summary of the transcript). You should circulate (e.g., email) to potential participants prior to training day. You will need to submit a copy of this page when you request certificates.

Monitoring Attendance

You must monitor individual participant attendance at “group live” programs to assign the correct number of CPE credits. A participant’s self-certification of attendance alone is not sufficient.

Use the **attendance sheet**. This lists the instructor(s) name and credentials, as well as the first and last name of each participant attending the seminar. The participant is expected to initial the sheet for their morning attendance and provide their signature for their afternoon attendance. If a participant arrives late, leaves early, or is a “no show,” the actual hours they

attended should be documented on the sign-in sheet and will be reflected on the participant's CPE certificate.

Real Time Instructor During Program Presentation

"Group live" programs must have a **qualified, real time instructor while the program is being presented**. Program participants must be able to interact with the instructor while the course is in progress (including the opportunity to ask questions and receive answers during the presentation).

Elements of Engagement

A "group live" program must include at least one element of engagement related to course content during each credit of CPE (for example, group discussion, polling questions, instructor-posed question with time for participant reflection, or use of a case study with different engagement elements throughout the program).

Make-Up Sessions

Individuals who are unable to attend the group study session may use the program materials for self-study either in print or online.

- If the print materials are used, the user should read the materials, watch the video, and answer the quizzer questions on the CPE Quizzer Answer Sheet. Send the answer sheet and course evaluation to the address listed on the answer sheet and the CPE certificate will be mailed or emailed to the user. Detailed instructions are provided on Network Program Self-Study Options.
- If the online materials are used, the user should log on to her/his individual Checkpoint Learning account to read the materials, watch the interviews, and answer the quizzer questions. The user will be able to print her/his/their CPE certificate upon completion of the quizzer. (If you need help setting up individual user accounts, please contact your firm administrator or customer service.)

Awarding CPE Certificates

The CPE certificate is the participant's record of attendance and is awarded by Checkpoint Learning Network after the "group live" documentation is received (and providing the course is delivered as 3 CPE credits). The certificate of completion will reflect the credit hours earned by the individual, with special calculation of credits for those who arrived late or left early.

Subscriber Survey Evaluation Forms

Use the evaluation form. You must include a means for evaluating quality. At the conclusion of the "group live" session, evaluations should be distributed and any that are completed are collected from participants. Those evaluations that are completed by participants should be returned to Checkpoint Learning Network along with the other course materials. While it is required that you circulate the evaluation form to all participants, it is NOT required that the participants fill it out. A preprinted evaluation form is included in the transcript each month for your convenience.

Retention of Records

Regardless of whether Checkpoint Learning Network is the sponsor for the "group live" session, it is required that the firm hosting the "group live" session retain the following information for a period of five years from the date the program is completed unless state law dictates otherwise:

- Record of participation (Group Study Attendance sheets; indicating any late arrivals and/or early departures)
- Copy of the program materials
- Timed agenda with topics covered and elements of engagement used
- Date and location of course presentation
- Number of CPE credits and field of study breakdown earned by participants
- Instructor name and credentials
- Results of program evaluations.

Finding the Transcript

When the DVD is inserted into a DVD drive, the video will immediately begin to play and the menu screen will pop up, taking the entire screen. Hitting the Esc key should minimize it to a smaller window. To locate the pdf file of the transcript either to save or email to others, go to the start button on the computer. In My Computer, open the drive with the DVD. The Adobe Acrobat files are the transcript files. If you do not currently have Adobe Acrobat Reader (Mac versions of the reader are also available), a free version of the reader may be downloaded at:

- <https://get.adobe.com/reader/>

Requesting Participant CPE Certificates

When delivered as 3 CPE credits, documentation of your “group live” session should be sent to Checkpoint Learning Network by one of the following means:

Mail: Thomson Reuters
PO Box 115008
Carrollton, TX 75011-5008

Email: CPLgrading@tr.com

Fax: 888.286.9070

When sending your package to Thomson Reuters, you must include ALL of the following items:

Form Name	Included?	Notes
Advertising / Promotional Page		Complete this form and circulate to your audience before the training event.
Attendance Sheet		Use this form to track attendance during your training session.
Subscriber Survey Evaluation Form		Circulate the evaluation form at the end of your training session so that participants can review and comment on the training. Return to Thomson Reuters any evaluations that were completed. You do not have to return an evaluation for every participant.

Incomplete submissions will be returned to you.

“Group Internet Based” Format

CPE Credit

All CPE Network products are developed and intended to be delivered as 3 CPE credits. You should allocate sufficient time in your delivery so that there is no less than 2.5 clock hours:

50 minutes per CPE credit TIMES 3 credits = 150 minutes = 2.5 clock hours

If you wish to have a break during your training session, you should increase the length of the training beyond 2.5 hours as necessary. For example, you may wish to schedule your training from 9 AM to 12 PM and provide a ½ hour break from 10:15 to 10:45.

***Effective November 1, 2018:** Checkpoint Learning CPE Network products ‘group live’ sessions must be delivered as 3 CPE credits and accredited to the field(s) of study as designated by Checkpoint Learning Network. Checkpoint Learning Network will not issue certificates for “group live” deliveries of less than 3 CPE credits (unless the course was delivered as 3 credits and there are partial credit exceptions (such as late arrivals and early departures). Therefore, if you decide to deliver the “group live” session with less than 3 CPE credits, your firm will be the sponsor as Checkpoint Learning Network will not issue certificates to your participants.

Advertising / Promotional Page

Create a promotion page (use the template following the executive summary in the transcript). You should circulate (e.g., email) to potential participants prior to training day. You will need to submit a copy of this page when you request certificates.

Monitoring Attendance in a Webinar

You must monitor individual participant attendance at “group internet based” programs to assign the correct number of CPE credits. A participant’s self-certification of attendance alone is not sufficient.

Use the **Webinar Delivery Tracking Report**. This form lists the moderator(s) name and credentials, as well as the first and last name of each participant attending the seminar. During a webinar you must set up a monitoring mechanism (or polling mechanism) to periodically check the participants’ engagement throughout the delivery of the program.

In order for CPE credit to be granted, you must confirm the presence of each participant **3 times per CPE hour and the participant must reply to the polling question**. Participants that respond to less than 3 polling questions in a CPE hour will not be granted CPE credit. For example, if a participant only replies to 2 of the 3 polling questions in the first CPE hour, credit for the first CPE hour will not be granted. (Refer to the Webinar Delivery Tracking Report for examples.)

Examples of polling questions:

1. You are using **Zoom** for your webinar. The moderator pauses approximately every 15 minutes and ask that participants confirm their attendance by using the “raise hands” feature. Once the participants raise their hands, the moderator records the participants who have their hands up in the **webinar delivery tracking report** by putting a YES in the webinar delivery tracking report. After documenting in the spreadsheet, the instructor (or moderator) drops everyone’s hands and continues the training.
2. You are using **Teams** for your webinar. The moderator will pause approximately every 15 minutes and ask that participants confirm their attendance by typing “Present” into the Teams chat box. The moderator records the participants who have entered “Present” into the chat box into the **webinar delivery tracking report**. After documenting in the spreadsheet, the instructor (or moderator) continues the training.
3. If you are using an application that has a way to automatically send out polling questions to the participants, you can use that application/mechanism. However, following the event, you should create a **webinar delivery tracking report** from your app’s report.

Additional Notes on Monitoring Mechanisms:

1. The monitoring mechanism does not have to be “content specific.” Rather, the intention is to ensure that the remote participants are present and paying attention to the training.
2. You should only give a minute or so for each participant to reply to the prompt. If, after a minute, a participant does not reply to the prompt, you should put a NO in the webinar delivery tracking report.
3. While this process may seem unwieldy at first, it is a required element that sponsors must adhere to. And after some practice, it should not cause any significant disruption to the training session.
4. **You must include the Webinar Delivery Tracking report with your course submission if you are requesting certificates of completion for a “group internet based” delivery format.**

Real Time Moderator During Program Presentation

“Group internet based” programs must have a **qualified, real time moderator while the program is being presented**. Program participants must be able to interact with the moderator while the course is in progress (including the opportunity to ask questions and receive answers

during the presentation). This can be achieved via the webinar chat box, and/or by unmuting participants and allowing them to speak directly to the moderator.

Make-Up Sessions

Individuals who are unable to attend the “group internet based” session may use the program materials for self-study either in print or online.

- If print materials are used, the user should read the materials, watch the video, and answer the quizzer questions on the CPE Quizzer Answer Sheet. Send the answer sheet and course evaluation to the address listed on the answer sheet and the CPE certificate will be mailed or emailed to the user. Detailed instructions are provided on Network Program Self-Study Options.
- If the online materials are used, the user should log on to her/his individual Checkpoint Learning account to read the materials, watch the interviews, and answer the quizzer questions. The user will be able to print her/his CPE certificate upon completion of the quizzer. (If you need help setting up individual user accounts, please contact your firm administrator or customer service.)

Awarding CPE Certificates

The CPE certificate is the participant’s record of attendance and is awarded by Checkpoint Learning Network after the “group internet based” documentation is received (and providing the course is delivered as 3 CPE credits). The certificate of completion will reflect the credit hours earned by the individual, with special calculation of credits for those who may not have answered the required amount of polling questions.

Subscriber Survey Evaluation Forms

Use the evaluation form. You must include a means for evaluating quality. At the conclusion of the “group live” session, evaluations should be distributed and any that are completed are collected from participants. Those evaluations that are completed by participants should be returned to Checkpoint Learning Network along with the other course materials. While it is required that you circulate the evaluation form to all participants, it is NOT required that the participants fill it out. A preprinted evaluation form is included in the transcript each month for your convenience.

Retention of Records

Regardless of whether Checkpoint Learning Network is the sponsor for the “group internet based” session, it is required that the firm hosting the session retain the following information for a period of five years from the date the program is completed unless state law dictates otherwise:

- Record of participation (Webinar Delivery Tracking Report)
- Copy of the program materials
- Timed agenda with topics covered
- Date and location (which would be “virtual”) of course presentation
- Number of CPE credits and field of study breakdown earned by participants
- Instructor name and credentials
- Results of program evaluations

Finding the Transcript

When the DVD is inserted into a DVD drive, the video will immediately begin to play and the menu screen will pop up, taking the entire screen. Hitting the Esc key should minimize it to a smaller window. To locate the pdf file of the transcript either to save or email to others, go to the start button on the computer. In My Computer, open the drive with the DVD. It should look something like the screenshot below. The Adobe Acrobat files are the transcript files. If you do not currently have Adobe Acrobat Reader (Mac versions of the reader are also available), a free version of the reader may be downloaded at:

- <https://get.adobe.com/reader/>

Alternatively, for those without a DVD drive, the email sent to administrators each month has a link to the pdf for the newsletter. The email may be forwarded to participants who may download the materials or print them as needed.

Requesting Participant CPE Certificates

When delivered as 3 CPE credits, documentation of your “group internet based” session should be sent to Checkpoint Learning Network by one of the following means:

Mail: Thomson Reuters
PO Box 115008
Carrollton, TX 75011-5008

Email: CPLgrading@tr.com

Fax: 888.286.9070

When sending your package to Thomson Reuters, you must include ALL the following items:

Form Name	Included?	Notes
Advertising / Promotional Page		Complete this form and circulate to your audience before the training event.
Webinar Delivery Tracking Report		Use this form to track the attendance (i.e., polling questions) during your training webinar.
Evaluation Form		Circulate the evaluation form at the end of your training session so that participants can review and comment on the training. Return to Thomson Reuters any evaluations that were completed. You do not have to return an evaluation for every participant.

Incomplete submissions will be returned to you.

“Self-Study” Format

If you are unable to attend the live group study session, we offer two options for you to complete your Network Report program.

Self-Study—Print

Follow these simple steps to use the printed transcript and DVD:

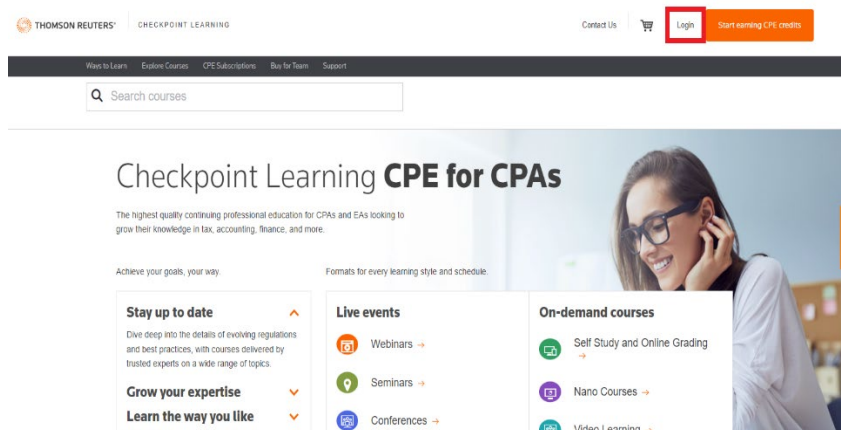
- Watch the DVD.
- Review the supplemental materials.
- Read the discussion problems and the suggested answers.
- Complete the quizzer by filling out the bubble sheet enclosed with the transcript package.
- Complete the survey. We welcome your feedback and suggestions for topics of interest to you.
- Mail your completed quizzer and survey to:

Thomson Reuters
PO Box 115008
Carrollton, TX 75011-5008

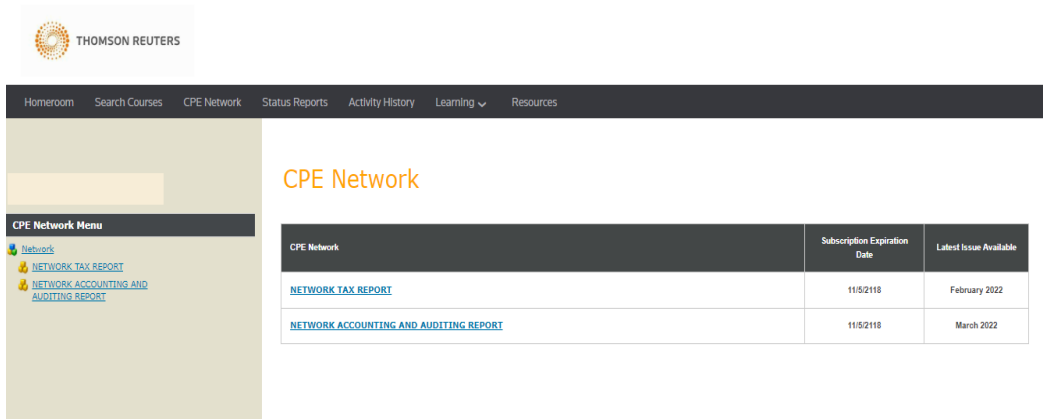
Self-Study—Online

Follow these simple steps to use the online program:

- Go to www.checkpointlearning.thomsonreuters.com.
- Log in using your username and password assigned by your firm’s administrator in the upper right-hand margin (“Login or Register”).

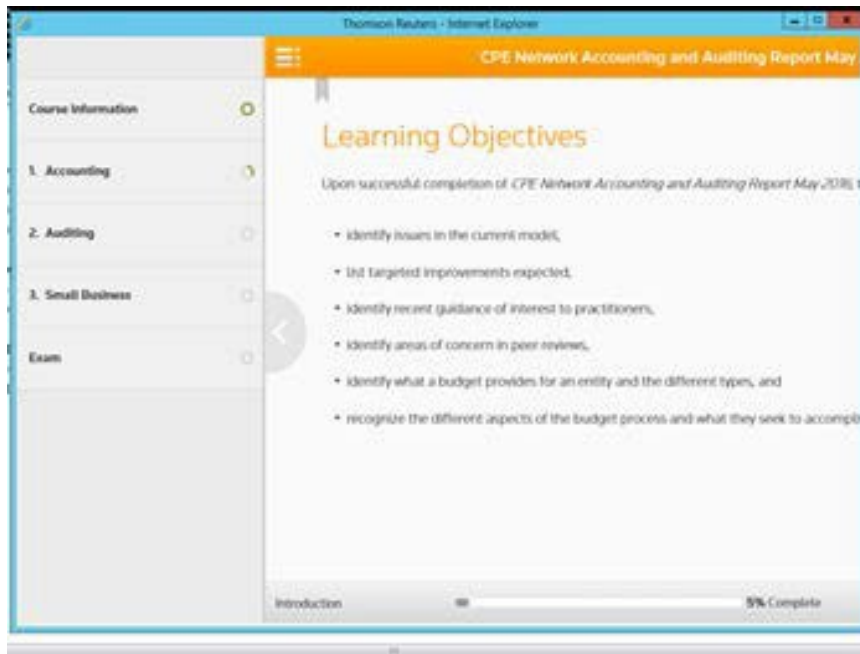


- In the **CPE Network** tab, select the desired Network Report and then the appropriate edition.



CPE Network	Subscription Expiration Date	Latest Issue Available
NETWORK TAX REPORT	11/5/2118	February 2022
NETWORK ACCOUNTING AND AUDITING REPORT	11/5/2118	March 2022

The Chapter Menu is in the gray bar at the left of your screen:



Thomson Reuters - Internet Explorer

CPE Network Accounting and Auditing Report May 2018

Learning Objectives

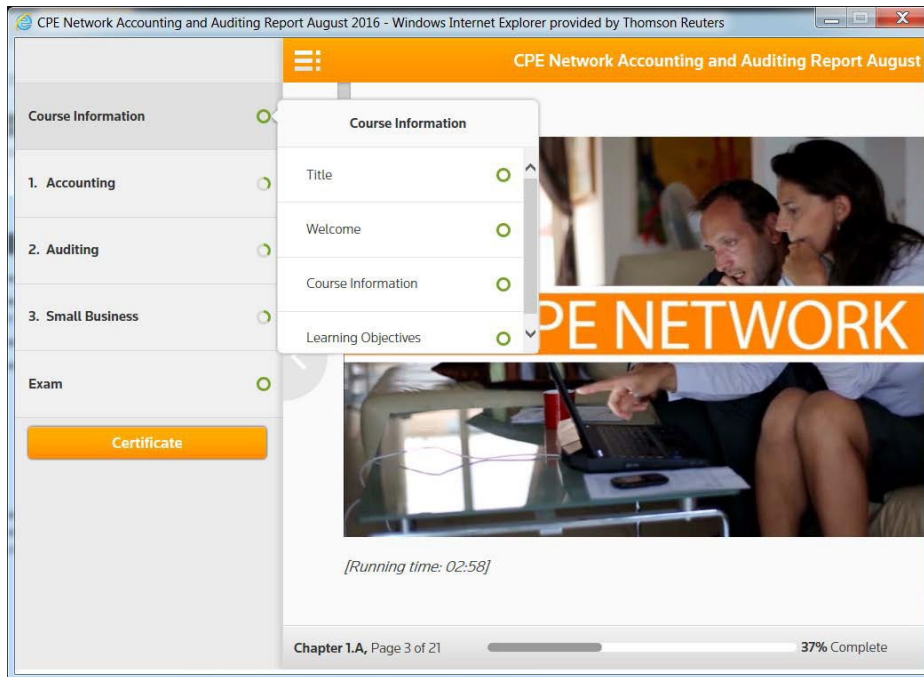
Upon successful completion of *CPE Network Accounting and Auditing Report May 2018*:

- identify issues in the current model;
- list targeted improvements expected;
- identify recent guidance of interest to practitioners;
- identify areas of concern in peer reviews;
- identify what a budget provides for an entity and the different types; and
- recognize the different aspects of the budget process and what they seek to accomplish

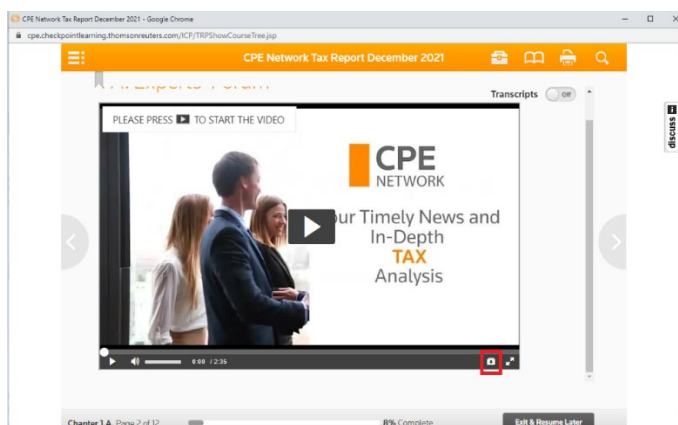
Introduction 5% Complete

Click down to access the dropdown menu and move between the program Chapters.

- **Course Information** is the course Overview, including information about the authors and the program learning objectives



- **Each Chapter is now self-contained.** Years ago, when on the CPEasy site, the interview segments were all together, then all the supplemental materials, etc. Today, each chapter contains the executive summary and learning objectives for that segment, followed by the interview, the related supplemental materials, and then the discussion questions. This more streamlined approach allows administrators and users to more easily access the related materials.



Video segments may be downloaded from the CPL player by clicking on the download button. Tip: you may need to scroll down to see the download button.

Thomson Reuters - Internet Explorer

CPE Network Accounting and Auditing Report May 2016

Transcripts ☒

Chapter 1 Liabilities and Equity: Another Look at the Model

Both the FASB and the AICPA have targeted improvements to the guidance related to liabilities and equity instruments. The current debt-equity model in U.S. GAAP is very complex, making it difficult for both preparers and accountants to implement.

For more on the targeted improvements in this area, let's join Paul Munter, professor in practice for the University of Colorado at Boulder, and CPE Network's Debi Grove Casey.

Ms. Grove Casey

Today, we want to talk a little bit

Please note that the transcript [Liabilities and Equity Transcripts](#) can also be found as a link and in the Tools section.

Chapter 1A, Page 4 of 21 8% Complete [Exit & Resume Later](#)

Transcripts for the interview segments can be viewed at the right side of the screen via a toggle button at the top labeled **Transcripts** or via the link to the pdf below the video (also available in the toolbox in the resources section). The pdf will appear in a separate pop-up window.

D:\xml\production\working\U6015494\N... Network Accounting and Auditing Report May 2016

Transcripts ☒

Chapter 1 Liabilities and Equity: Another Look at the Model

Both the FASB and the AICPA have targeted improvements to the guidance related to liabilities and equity instruments. The current debt-equity model in U.S. GAAP is very complex, making it difficult for both preparers and accountants to implement.

For more on the targeted improvements in this area, let's join Paul Munter, professor in practice for the University of Colorado at Boulder, and CPE Network's Debi Grove Casey.

Ms. Grove Casey

Today, we want to talk a little bit

Please note that the transcript [Liabilities and Equity Transcripts](#) can also be found as a link and in the Tools section.

Chapter 1A, Page 4 of 21 8% Complete [Exit & Resume Later](#)

CHAPTER 1A: ACCOUNTING

Liabilities and Equity: Another Look at the Model

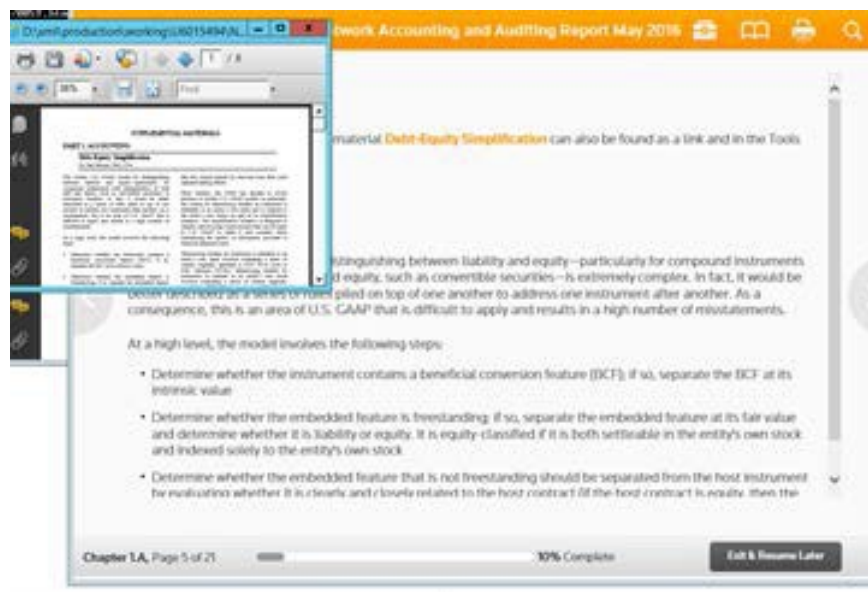
Both the FASB and the AICPA have targeted improvements to the guidance related to liabilities and equity instruments. The current debt-equity model in U.S. GAAP is very complex, making it difficult for both preparers and accountants to implement.

For more on the targeted improvements in this area, let's join Paul Munter, professor in practice for the University of Colorado at Boulder, and CPE Network's Debi Grove Casey.

Ms. Grove Casey

Today, we want to talk a little bit

Click the arrow at the bottom of the video to play it, or click the arrow to the right side of the screen to advance to the supplemental material. As with the transcripts, the supplemental materials are also available via the toolbox and the link will pop up the pdf version in a separate window.



Continuing to click the arrow to the right side of the screen will bring the user to the Discussion problems related to the segment.

The Suggested Answers to the Discussion Problems follow the Discussion Problems.

The screenshot shows a web interface for the CPE Network Accounting and Auditing Report July 2016. The header is orange with a menu icon, title, and icons for home, books, printer, and search. The main content area is titled "Suggested Answers to Discussion Problems" and contains three numbered items. Item 1 lists three categories: Held-to-maturity, Trading, and Available-for-sale, followed by a paragraph explaining the classification process. Item 2 describes the trading securities category. Item 3 discusses impairment recognition. The footer shows "Chapter 3.A, Page 20 of 20", a progress bar at 100% Complete, and an "Exit & Resume Later" button.

Suggested Answers to Discussion Problems

1. ASC 320 requires that, at acquisition, an enterprise classify debt and marketable equity securities into one of three categories:
 - Held-to-maturity
 - Trading
 - Available-for-sale

An entity decides how to classify securities based on its intended holding period for each individual security, using the framework in ASC 320. In establishing its intent, an entity should consider relevant trends and experience, such as previous sales and transfers of securities. Classification decisions should be made at acquisition and, preferably, formally documented. It is not appropriate to use "hindsight" to classify securities transactions, perhaps by considering changes in value after acquisition.
2. The trading securities category includes securities that are bought and held principally for the purpose of selling them in the short term. Trading generally reflects active and frequent buying and selling, and trading securities are generally used with the objective of generating profits on short-term differences in price. "Short-term," in this context, is intended to be measured in hours and days, rather than in months or years, according to ASC 320. However, an entity is not precluded from classifying as trading a security it plans to hold for a longer period, as long as that designation occurs at acquisition.
3. Impairment is recognized in earnings when a decline in value has occurred that is deemed to be other than temporary, and the current fair value becomes the new cost basis for the security. An investment is considered to be impaired if the fair value of the investment is less than its cost basis. Cost includes adjustments made for

Chapter 3.A, Page 20 of 20 100% Complete Exit & Resume Later

The **Exam** is accessed by clicking the last gray bar on the menu at the left of the screen or clicking through to it. Click the orange button to begin.

When you have completed the quizzer, click the button labeled **Grade** or the **Review** button.

The screenshot shows a web interface for the CPE Network Accounting and Auditing Report June 2016. The header is orange with a menu icon, title, and icons for home, books, printer, and search. The main content area is titled "Course Exams Completed" and contains a message stating the exam is completed. It then provides instructions and two orange buttons: "Review My Answers" and "Grade My Answers". The footer shows "Course, Completed", a progress bar at 100% Complete, and an "Exit & Resume Later" button.

Course Exams Completed

You have completed the exam for this course.

Please choose your next course of action by selecting on one of the buttons below.

"Review My Answers" will take you back through exam, giving you the opportunity to make changes.

Review My Answers

"Grade My Answers" will result in providing you with a final score for this course.

Grade My Answers

Course, Completed 100% Complete Exit & Resume Later

- Click the button labeled **Certificate** to print your CPE certificate.
- The final quizzer grade is displayed and you may view the graded answers by clicking the button labeled **view graded answer**.

Additional Features Search

Checkpoint Learning offers powerful search options. Click the **magnifying glass** at the upper right of the screen to begin your search. Enter your choice in the **Search For:** box.

Search Results are displayed with the number of hits.

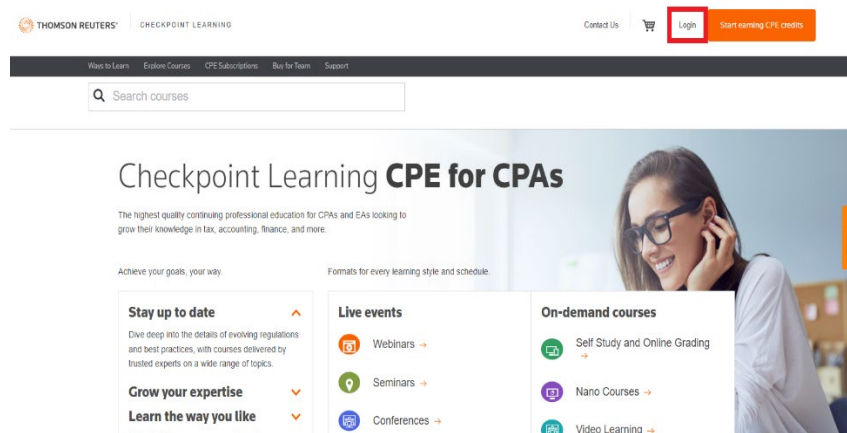
Print

To display the print menu, click the printer icon in the upper bar of your screen. You can print the entire course, the transcript, the glossary, all resources, or selected portions of the course. Click your choice and click the orange **Print**.

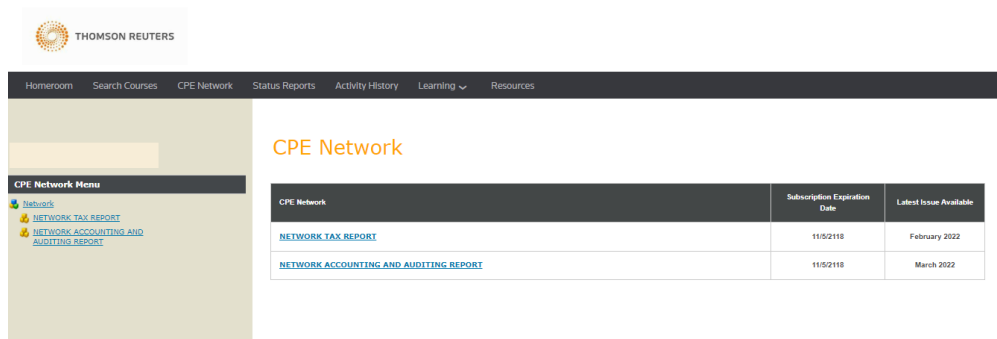
Transitioning From DVDs

Follow these simple steps to access the video and pdf for download from the online platform:

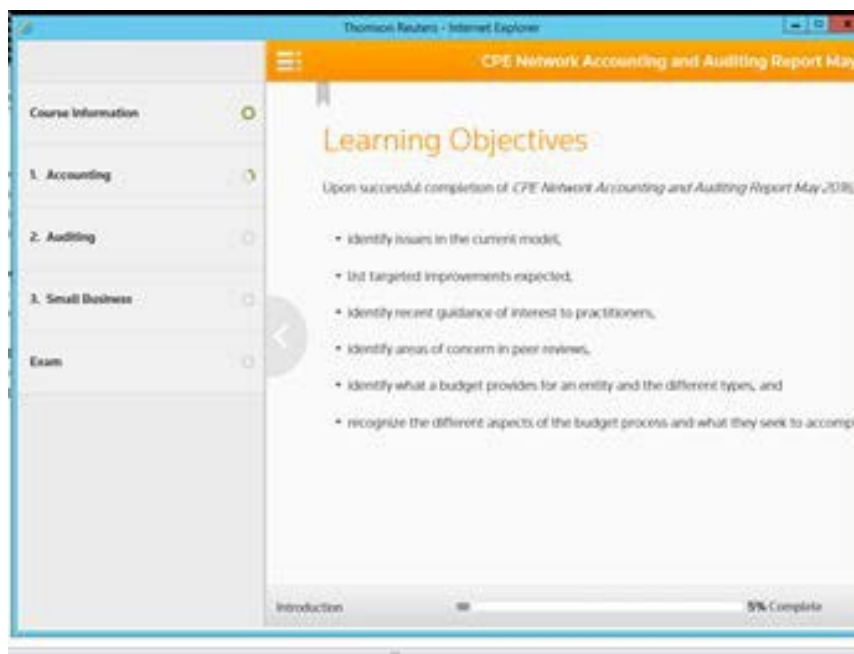
- Go to www.checkpointlearning.thomsonreuters.com .
- Log in using your username and password assigned by your firm’s administrator in the upper right-hand margin (“Login or Register”).



- In the CPE **Network** tab, select the desired Network Report by clicking on the title, then select the appropriate edition.

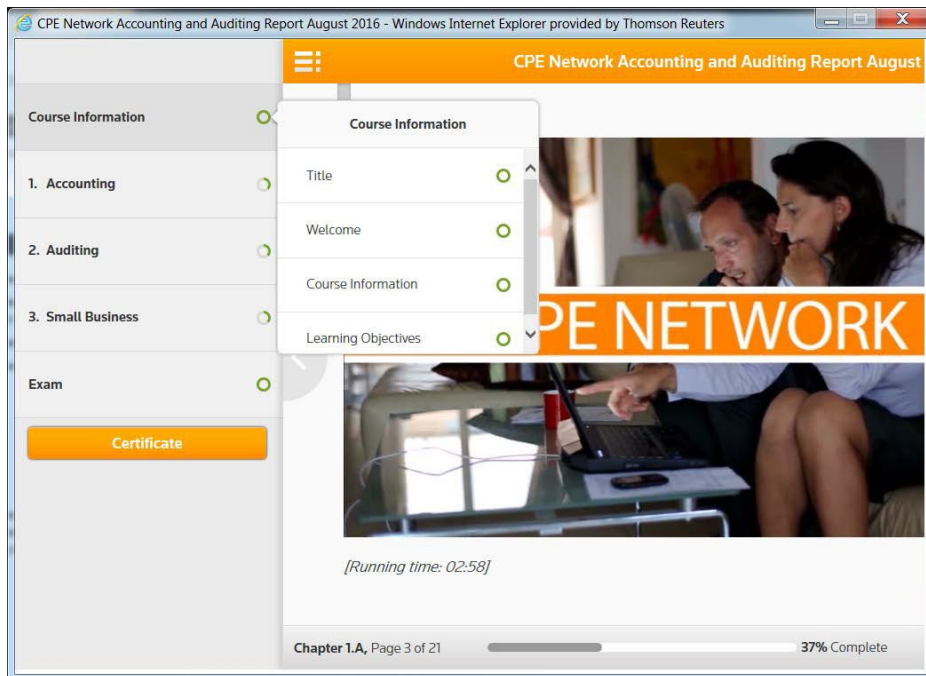


The Chapter Menu is in the gray bar at the left of your screen:



Click down to access the dropdown menu and move between the program Chapters.

- **Course Information** is the course Overview, including information about the authors and the program learning objectives



- Each Chapter is self-contained. Each chapter contains the executive summary and learning objectives for that segment, followed by the interview, the related supplemental materials, and then the discussion questions.



Video segments may be downloaded from the CPL player by clicking on the download button noted above. Tip: You may need to use the scroll bar to the right of the video to see the download button.

PDFs may be downloaded from either the course toolbox in the upper right corner of the Checkpoint Learning screen or from the email sent by Checkpoint Learning CPE Customer Service.

What Does It Mean to Be a CPE Sponsor?

If your organization chooses to vary from the instructions outlined in this User Guide, your firm will become the CPE Sponsor for this monthly series. The sponsor rules and requirements noted below are only highlights and reflect those of NASBA, the national body that sets guidance for development, presentation, and documentation for CPE programs. **For any specific questions about state sponsor requirements, please contact your state board. They are the final authority regarding CPE Sponsor requirements.** Generally, the following responsibilities are required of the sponsor:

- Arrange for a location for the presentation
- Advertise the course to your anticipated participants and disclose significant features of the program in advance
- Set the start time
- Establish participant sign-in procedures
- Coordinate audio-visual requirements with the facilitator
- Arrange appropriate breaks
- Have a real-time instructor during program presentation
- Ensure that the instructor delivers and documents elements of engagement
- Monitor participant attendance (make notations of late arrivals, early departures, and “no shows”)
- Solicit course evaluations from participants
- Award CPE credit and issue certificates of completion
- Retain records for five years

The following information includes instructions and generic forms to assist you in fulfilling your responsibilities as program sponsor.

CPE Sponsor Requirements

Determining CPE Credit Increments

Sponsored seminars are measured by program length, with one 50-minute period equal to one CPE credit. One-half CPE credit increments (equal to 25 minutes) are permitted after the first credit has been earned. Sponsors must monitor the program length and the participants' attendance in order to award the appropriate number of CPE credits.

Program Presentation

CPE program sponsors must provide descriptive materials that enable CPAs to assess the appropriateness of learning activities. CPE program sponsors must make the following information available in advance:

- Learning objectives.
- Instructional delivery methods.
- Recommended CPE credit and recommended field of study.
- Prerequisites.
- Program level.
- Advance preparation.
- Program description.
- Course registration and, where applicable, attendance requirements.
- Refund policy for courses sold for a fee/cancellation policy.
- Complaint resolution policy.
- Official NASBA sponsor statement, if an approved NASBA sponsor (explaining final authority of acceptance of CPE credits).

Disclose Significant Features of Program in Advance

For potential participants to effectively plan their CPE, the program sponsor must disclose the significant features of the program in advance (e.g., through the use of brochures, website, electronic notices, invitations, direct mail, or other announcements). When CPE programs are offered in conjunction with non-educational activities, or when several CPE programs are offered concurrently, participants must receive an appropriate schedule of events indicating those components that are recommended for CPE credit. The CPE program sponsor's registration and attendance policies and procedures must be formalized, published, and made available to participants and include refund/cancellation policies as well as complaint resolution policies.

Monitor Attendance

While it is the participant's responsibility to report the appropriate number of credits earned, CPE program sponsors must maintain a process to monitor individual attendance at group programs to assign the correct number of CPE credits. A participant's self-certification of attendance alone is not sufficient. The sign-in sheet should list the names of each instructor and her/his credentials, as well as the name of each participant attending the seminar. The participant is expected to initial the sheet for their morning attendance and provide their signature for their afternoon attendance. If a participant leaves early, the hours they attended should be documented on the sign-in sheet and on the participant's CPE certificate.

Real Time Instructor During Program Presentation

“Group live” programs must have a qualified, real time instructor while the program is being presented. Program participants must be able to interact with the real time instructor while the course is in progress (including the opportunity to ask questions and receive answers during the presentation).

Elements of Engagement

A “group live” program must include at least one element of engagement related to course content during each credit of CPE (for example, group discussion, polling questions, instructor-posed question with time for participant reflection, or use of a case study with different engagement elements throughout the program).

Awarding CPE Certificates

The CPE certificate is the participant’s record of attendance and is awarded at the conclusion of the seminar. It should reflect the credit hours earned by the individual, with special calculation of credits for those who arrived late or left early. Attached is a sample *Certificate of Attendance* you may use for your convenience.

CFP credit is available if the firm registers with the CFP board as a sponsor and meets the CFP board requirements. IRS credit is available only if the firm registers with the IRS as a sponsor and satisfies their requirements.

Seminar Quality Evaluations for Firm Sponsor

NASBA requires the seminar to include a means for evaluating quality. At the seminar conclusion, evaluations should be solicited from participants and retained by the sponsor for five years. The following statements are required on the evaluation and are used to determine whether:

1. Stated learning objectives were met.
2. Prerequisite requirements were appropriate.
3. Program materials were accurate.
4. Program materials were relevant and contributed to the achievement of the learning objectives.
5. Time allotted to the learning activity was appropriate.
6. Individual instructors were effective.
7. Facilities and/or technological equipment were appropriate.
8. Handout or advance preparation materials were satisfactory.
9. Audio and video materials were effective.

You may use the enclosed preprinted evaluation forms for your convenience.

Retention of Records

The seminar sponsor is required to retain the following information for a period of five years from the date the program is completed unless state law dictates otherwise:

- Record of participation (the original sign-in sheets, now in an editable, electronic signable format)
- Copy of the program materials
- Timed agenda with topics covered and elements of engagement used
- Date and location of course presentation
- Number of CPE credits and field of study breakdown earned by participants
- Instructor name(s) and credentials
- Results of program evaluations

Appendix: Forms

Here are the forms noted above and how to get access to them.

Delivery Method	Form Name	Location	Notes
“Group Live” / “Group Internet Based”	Advertising / Promotional Page	Transcript	Complete this form and circulate to your audience before the training event.
“Group Live”	Attendance Sheet	Transcript	Use this form to track attendance during your training session.
“Group Internet Based”	Webinar Delivery Tracking Report	Transcript	Use this form to track the ‘polling questions’ which are required to monitor attendance during your webinar.
“Group Live” / “Group Internet Based”	Evaluation Form	Transcript	Circulate the evaluation form at the end of your training session so that participants can review and comment on the training.
Self Study	CPE Quizzer Answer Sheet	Transcript	Use this form to record your answers to the quiz.

Getting Help

Should you need support or assistance with your account, please see below:

Support Group	Phone Number	Email Address	Typical Issues/Questions
Technical Support	800.431.9025 (follow option prompts)	checkpointlearning.techsupport@thomsonreuters.com	<ul style="list-style-type: none">• Browser-based• Certificate discrepancies• Accessing courses• Migration questions• Feed issues
Product Support	800.431.9025 (follow option prompts)	checkpointlearning.productsupport@thomsonreuters.com	<ul style="list-style-type: none">• Functionality (how to use, where to find)• Content questions• Login Assistance
Customer Support	800.431.9025 (follow option prompts)	checkpointlearning.cpecustomerservice@thomsonreuters.com	<ul style="list-style-type: none">• Billing• Existing orders• Cancellations• Webinars• Certificates