

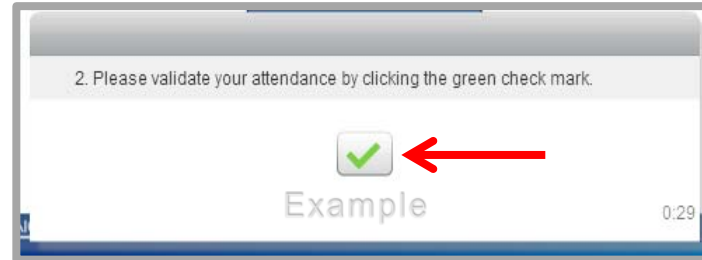


Technology Basics for Nonprofits

Earning CPE



- Disable all pop up blockers
- Any answer counts towards CPE credit
- Earn credit by responding to 75% of these pop-ups
- Click the CPE button at the end of this webcast
- A post event email with CPE information will be sent to you



Per NASBA, you cannot earn CPE credit by watching the archive of this webcast.

More Helpful Hints



Adjust your volume

- Click this blue button to adjust your volume.
- Be sure your computer's sound is turned on as well.



Ask your questions

- Feel free to submit content related questions to the speaker by clicking this button.
- Someone is available to assist with your technology and CPE related questions as well.



Download your materials

- Access today's slides and learning materials by clicking this download button at any time during this presentation
- If you need help accessing these materials send a message through the Q&A application

Today's Presenters



Cheryl R. Olson, CPA, CGMA

- Nonprofit Solutions Strategist
- Clark Nuber PS



Michael Forster, CPA, CGMA

- Chief Operating Officer
- The Wilson Center



Steve Vasconcellos, CPA, CGEIT

- Principal
- Clark Nuber PS

Learning Objectives

- Identify general and new technology definitions and terminology.
- Determine what to focus on in building ideal infrastructure for your organization.
- Identify compliance areas to pay attention to and stay current on.

“Everybody gets so much information all day long that they lose their common sense.”

- Gertrude Stein

Setting the Stage

- A not-for-profit is still a business and needs to be run as such
- Technology is a tool after focusing on people and process
- Make an investment of time and money

Definitions and Terminology

Blockchain

- **Blockchain** “is a system of distributed ledgers used to store records of transactions.”
- **Smart Contract** “is a computer program that directly controls the transfer of digital currencies or assets between parties under certain conditions.”
- **Virtual Currency** “is a type of unregulated, digital money, which is issued and usually controlled by its developers and used and accepted among the members of a specific virtual community.”



Definitions

- **Internet of Things** (IoT) is a network of devices such as vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data
- **Cloud Computing** is the delivery of computing services—servers, storage, databases, networking, software, analytics, intelligence and more—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale.
- **Cybersecurity** is the practice of protecting systems, networks, programs and people from digital attacks.
- **Artificial Intelligence** (AI) is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and other animals.

Definitions (continued)

- **Digital Transformation** is not necessarily about digital technology, but about the fact that technology, which is digital, allows people to solve their traditional problems. And they prefer this digital solution to the old solution
- **Technology Debt** is a concept in software development that reflects the implied cost of additional rework caused by choosing an easy solution now instead of using a better approach that would take longer.
- **Shadow IT** refers to information technology projects that are managed outside of, and without the knowledge of, the IT department

Acronyms

- **SaaS** (Software-as-a-Service) is a when a third-party provider hosts applications and makes them available to customers over the Internet. SaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).
- **IaaS** is a self-service model for accessing, monitoring and managing remote datacenter infrastructures, such as computing, storage, networking and networking services.
- **PaaS** provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure.
- **ML** (machine learning): Machine learning is the science of getting computers to act without being explicitly programmed. Machine learning is a subset of artificial intelligence.

Acronyms (continued)

- **Malware (Malicious Software)** is any software intentionally designed to cause damage. Viruses, worms, trojans, ransomware, and adware are all considered malware.
- **MFA (Multifactor Authentication)** is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
- **IAM (Identity and Access Management)** is the security discipline that enables individuals to access the right resources at the right times for the right reasons. The objective of IAM is to prove and manage your digital identity (the less there are, the easier to manage).

Building IT

IT Infrastructure

- Strategy
- People
- Process
- Technology



Strategy considerations in the new IT ‘world order’

New tools and services to protect – increased utilization of devices to perform our work from wireless-enabled laptops, to tablets, to smart phones; with varying OS’s and having ‘versioned’ APPS under BYOD policies

Increasing move to ‘cloud computing’ resulting in new organization to manage – “as a service” models; frequent technology releases can offer better/more options, but resource limits temper our appetite

New threats – the internet has opened numerous doors for bad things to happen; intruders and unauthorized users wreaking havoc

Strategy - operability dimensions

- Balancing the ever-changing and ever-increasing ways in which business transactions move across the financial platform.
- Determining how best to utilize cloud computing solutions; to donations accepted on-line thru websites, to credit cards accepted at the point of sale with wireless devices (and all things in between).
- Ensuring to capture, transmit, store and secure transaction data and business partner information (PII); all challenged by evolving business norms and the increasing number of vulnerabilities in our platform.

People – where is the talent?

- The Inherent question is do we “staff” talent or “contract” talent?
- The answer is that it depends!
- Considerations must be given to ‘functions’ and ‘factors’
- Trend shows that beginning in the 1990’s, companies began outsourcing functions at higher levels; this trend has only increased over the past 25 years.
- Business motives lean towards cost management, and scaling functions necessary to run the business that are not considered ‘core’ to the business



People – success of outsourced functions

According to Ted Beacon's summary in *Lean Outsourcing Blog* back in September, 2015:

- Outsourcing generally gets overall good success ratings.
- Spending on outsourcing is rising at a rate that is in step with IT operational spending as a whole.
- Increasingly organizations are outsourcing IT security work, web/e-commerce systems, and application hosting.



People - untrained users are costly

- Security ignorance compromises data
- Provide the training
- Rules of behavior
- Annual refresher training



Dimensions of security vs. safety

- **Security:** We must protect our computers and data in the same way that we secure the doors to our homes.
- **Safety:** We must behave in ways that protect us against risks and threats that come with technology.



People – importance of IT security

- ⦿ The internet allows an attacker to attack from anywhere on the planet.
- ⦿ Risks caused by poor security knowledge and practice:
 - Identity theft
 - Monetary theft
 - Legal ramifications (for yourself and companies)
 - Termination if company policies are not followed
- ⦿ According to multiple sources, the top vulnerabilities available for a cyber criminal are:
 - Web browser
 - IM clients
 - Web applications
 - Excessive user rights



Booming cyber crime industry

- Phishing and pharming thru social engineering
- Botnets: rent-a-botnet
- SPAM generators (steal email accounts and passwords – open for a ‘deeper dive’)
- Stolen sensitive information translates to \$\$\$\$\$
- Top 3 categories (noted by various sources):
 - Bank accounts – short-term access for small \$ amounts
 - Credit cards – mid-term access mid-size \$ amounts
 - Personal identities worth more – opening/sustaining false accounts

The reason “security” is paramount!

Breakdown of computer security

- A vulnerability is a point where a system is susceptible to attack.
- A threat is a possible danger to the system. The danger might be: 1) a person (a system cracker/intruder or a spy), 2) a thing (e.g. a faulty piece of equipment), or 3) an event (e.g. a fire or a flood) that might exploit a vulnerability of the system or the IT environment.
- Countermeasures are the techniques efforts implemented to protect the IT system and infrastructure.

Process – numerous considerations

- Infrastructure costs
- Staff costs
- Contractor costs
- Rising/uncertain data center costs
- Upgrades, customizations
- Legacy platforms (data portability considerations)
- Cost of entry/exit for a solution/upfront cost impact
- Pace of marketplace change
- Access to best practices

Side by side example of cost/ benefit trade-off

Traditional costs:

- Hardware (initial upfront)
- Software (initial upfront)
- Hardware repair/upgrades
- Software upgrades
- Staff costs
- Energy costs
- Training

Traditional limits:

- Maximum load
- Maximum up-time
- Maximum users
- MTTR (repair mean time)
- Dependencies

Cloud costs:

- Cost per user (spread out)
- Cost by bandwidth/storage
- Cost increase over time
- Cost of additional services
- Legal consultation costs
- Staff costs
- Training

Cloud limitations:

- Users
- Bandwidth
- Storage
- Service Support
- Dependencies



Technology

- Business requirements / Understand the benefit
 - Do this after people and process, technology becomes relevant (don't put the cart before the horse)
- Inventory
 - Have a list and values associated
- Owners
 - Strong accountability





Floating on a Cloud

The IT conundrum – what , how and how much?

One more definition - cloud computing – what is it?

- **Cloud computing** is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electric grid) over a network (typically the Internet); and can be provisioned and released with minimal management effort and service provider interactions.
- **Growing number of “as a service” formulations:**
 - Software as a Service (SaaS)
 - Infrastructure as a Service (IaaS)
 - Platform as a Service (PaaS)
 - Communications as a Service (Caas)
 - Network as a Service (NaaS)
 - Monitoring as a Service (MaaS)
 - Security as a Service (SECaaS)

“As a service” diagnostics

- TCO – generally better predictability of investment
- Costs are more evenly spread over the life of the system
- Link of investment to value
 - You pay as you go and grow
- Re-shaped risk (risk minimization framework)
- Upgrade availability – ‘buy-up’ menu options
- Constraints – “menu” limits your options!
 - This is often a good thing

Although “security” is paramount!

Monitor and evaluate metrics

- Did you solve your problem? Does the IT Solution meet the requirement?
- Metrics?
 - Business case is a living breathing document; updated over the life cycle of the project/solution

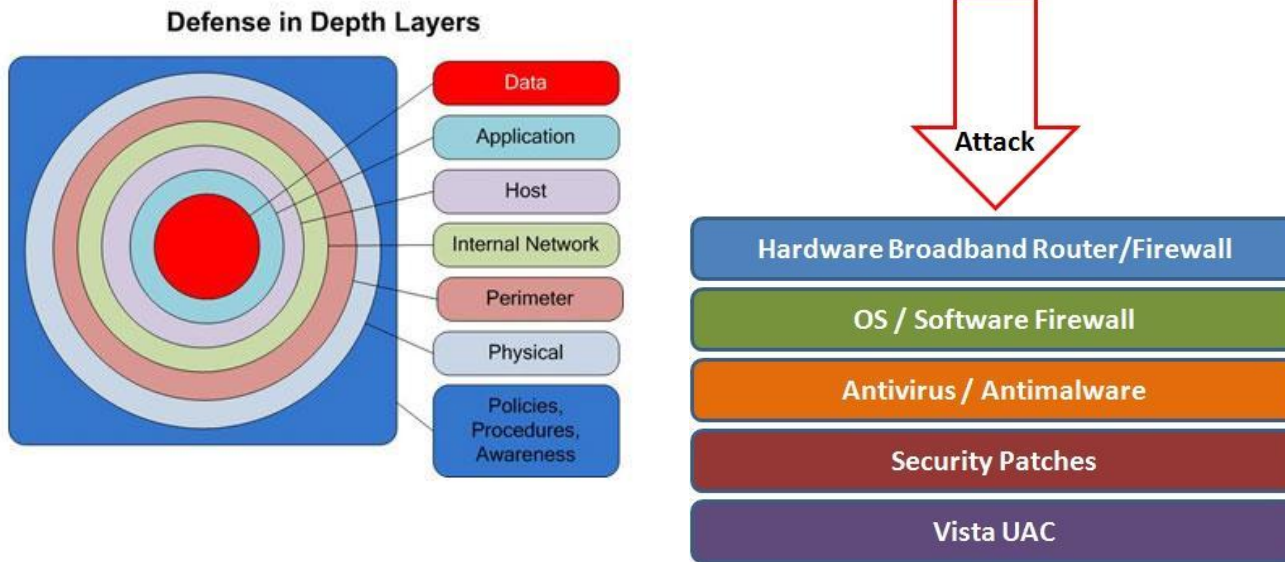
Goals of information technology

- Integrity:
 - Guarantee that the data is what we expect
- Confidentiality
 - The information must just be accessible to the authorized people
- Reliability
 - Computers should work without having unexpected problems
- Authentication
 - Guarantee that only authorized persons can access to the resources



Measurable defense

Defense in depth uses multiple layers of defense to address technical, personnel and operational issues.



Compliance areas

Regulatory compliance

- Organizations face an ever increasing list of compliance obligations, such as:

Regulation	Who Needs to Comply	Security Areas Covered
- SOX - Financial statement audits	US public/private/NFP entities	Defined to secure the public against corporate fraud/misrepresentation
PCI DSS <i>Payment Card Industry Data Security Standard</i>	Merchants who take credit cards	Privacy of customer financial data
GLBA <i>Gramm-Leach-Bliley Act</i>	US financial institutions	<ul style="list-style-type: none">- Privacy of personal information- Safety of internet based products & services- Other
COPPA <i>Children's Online Privacy Protection Act</i>	Entities (websites) storing data on children under 13	<ul style="list-style-type: none">- Parental consent- Privacy policy

Regulatory compliance (continued)

Regulation	Who Needs to Comply	Security Areas Covered
EU GDPR <i>General Data Protection Regulation</i>	Any organization holding personal data on EU citizens	Consumer privacy
Various State Privacy Laws <i>(i.e., California Consumer Privacy Act)</i>	Any entity storing or accessing private consumer data	Consumer privacy
HIPAA <i>Health Insurance Portability and Accountability Act</i>	US healthcare organizations	Creating, storing and transmitting electronic protected health information
HITECH <i>Health Information Technology for Economic and Clinical Health</i>	US healthcare organizations and their partners (business associates)	Similar to above but extends HIPAA requirements to third parties

Frameworks and policies

- **Technology (including security)** are common methods to satisfy a compliance requirement. A compliance requirement is the “what”.
- **A framework** of managing risk (including compliance and governance) is:
 - The “how” to demonstrate compliance
 - The method for organizations to think about the cost/benefit of accepting the risk versus addressing the risk
 - A way communicate this “how” in form of **policies**.
 - A way to show due diligence (a defensible position)

Frameworks and policies (continued)

- **Compliance is a business decision.** Frameworks help manage these decisions and eventually identify compliance requirements:
 - **Enterprise risk** refers to the risk that an organization won't meet its objectives. COSO is a good framework.
 - **IT risk** refers to the risk that IT won't deliver value in support of these objectives. A common framework is COBIT (and ITIL).
- For example, if an organization is determined to eradicate measles, an IT risk can be the risk that current IT systems are not equipped to adequately predict the next outbreak.
- Common outputs during the assessment of risk at the enterprise and IT levels include:
 - IT strategic plan
 - Business impact analysis

Frameworks and policies (continued)

- **IT security risk** is the risk that enterprise assets won't be optimally protected to support the mission/vision
 - NIST SP800-35, ISO 27001, ISO 27002, CIS-20 are common frameworks and controls
 - NIST SP800-30; Octave, RISK IT are common risk assessment guides
- For example, as a result of the IT risk, the organization chooses and implements a data tool that collects/analyzes patient data, geographic data and other data points
 - The relevant security controls must be selected and deployed to comply with HIPAA/HITECH
 - The controls must be cost-efficient – for example, if this tool is not accessible through a network, should an organization adopt network security controls?

Frameworks and policies (continued)

- **Common security-related policies:**
 - Business continuity plan / disaster recovery
 - IT security policy
 - Asset inventory
 - Data classification
 - Data retention



Security and financial statement audits

- As with most compliance requirements, security could also be part of financial statement audits
- Core security controls, also known as logical access helps enforce segregation of duties (authorization, record-keeping and custody of assets)
- Coupled with effective change management controls, strengthening IT controls can enable completeness and accuracy of financial data
- Other controls include backups, recovery and incident management controls
- The controls above are called IT general controls; inadequate design and operation of these controls may lead the auditor to ask: How can we trust the financial data in your system?

Conclusion

Top 6 things you definitely don't want to do

1. Ignore IT needs as they may have ideas
2. Get caught without governing IT policies
3. Not train staff on using the technology and the risks
4. Not provide oversight of technology vendors or volunteers, especially related to security
5. Buy next generation IT solutions without understanding the WHY behind them
6. Buy any solutions without determining your functional requirements

“The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.”

-Bill Gates

Top 6 things you should do

1. Investment in technology as a professional development area
2. Annual Pen Tests
3. Maintain and clean up your data
4. Get a handle on compliance, including contracts
5. Have insurance
6. Use mission, vision and strategy for your filter

“Without data,
you’re just another
person with an
opinion.”

-W. Edwards
Deming

Conclusion

- Determine which technology buzzwords apply to your organization
- Build and maintain the ideal technology infrastructure that is right for your organization
- Educate yourself and stay current on compliance and regulatory requirements

Resources

- Does your IT strategy align with your strategic plan?

https://www.accountingtoday.com/opinion/what-is-your-accounting-firms-it-strategy?utm_campaign=daily-dec%203%202018&utm_medium=email&utm_source=newsletter&eid=6f6e0691b79c7be1694a5e34928cec41

- Keeping Technology Safe When Someone Leaves Your Organization

https://netraising.com/resources/when-people-leave/?utm_medium=email&utm_campaign=NetRaising%20%20October%202018&utm_content=NetRaising%20%20October%202018+CID_78c95c086a4e84d0a58aa09728d59b5e&utm_source=CreateSend&utm_term=Read%20More

- 31 Tech Predictions for 2019

<https://www.inc.com/christina-desmarais/31-tech-predictions-for-2019.html>

Resources (continued)

- What is Blockchain

<https://www.simplybusiness.co.uk/knowledge/articles/2017/07/what-is-blockchain-and-how-does-it-work-a-beginners-guide/>

- 12 Common Technology Mistakes You Should Avoid

https://www.journalofaccountancy.com/issues/2019/jan/common-technology-mistakes.html?utm_source=ml:cpainsider&utm_medium=email&utm_campaign=07Jan2019

Resources (continued)

- AICPA Resources
 - Go Beyond Disruption <https://www.aicpa-cima.com/disruption.html>
 - Why cyberdefenses are worth the cost
<https://www.journalofaccountancy.com/issues/2018/nov/cyberdefense-for-not-for-profits.html>
 - Bitcoin Basics for NFPs: Accepting and Valuing Cryptocurrency Gifts
<https://www.aicpa.org/interestareas/notforprofit/resources/governancemanagement/bitcoin-basics-accepting-valuing-cryptocurrency-gifts.html>
 - Cryptocurrency Gift Strategies <https://www.journalofaccountancy.com/issues/2019/feb/cryptocurrency-gift-strategies-for-nfp.html>

Resources (continued)

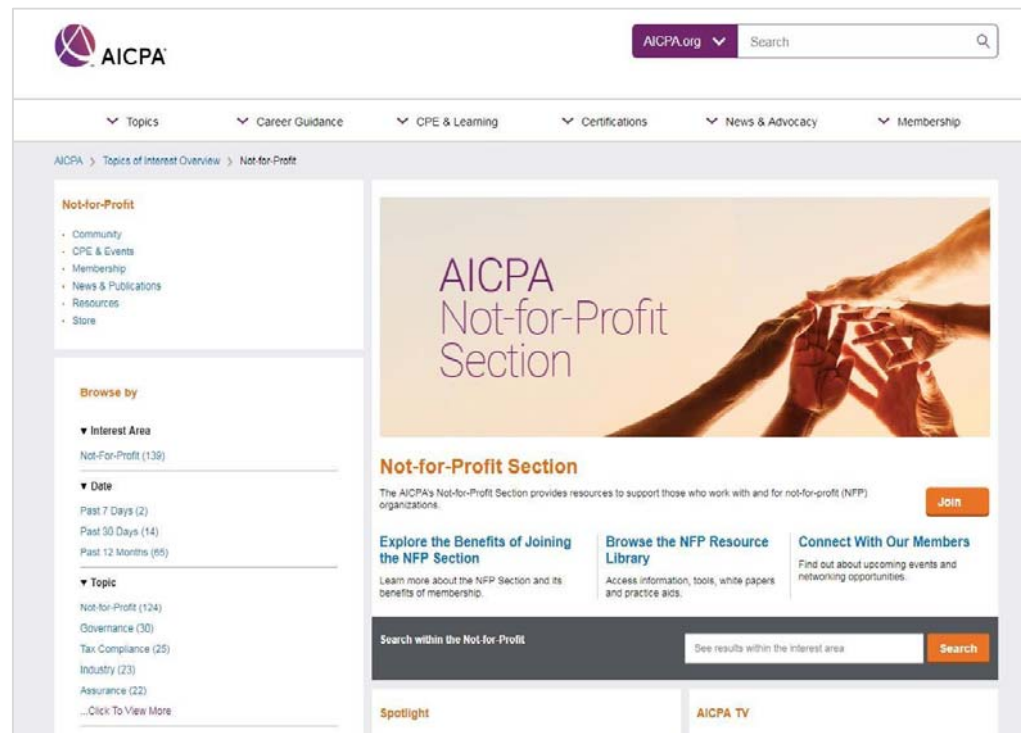
- AICPA locked resources for section members:
 - IT Controls for Not-for-Profit Entities <https://protect-us.mimecast.com/s/KqxiCPNW4ZCEprIS1F-bW?domain=aicpa.org>
 - Information Security Policy <https://protect-us.mimecast.com/s/mD-LCQWg40Fj0Exlkiix7?domain=aicpa.org>
- AICPA Areas
 - AICPA Information Management and Technology Assurance Resources <https://www.aicpa.org/interestareas/informationtechnology.html>
 - AICPA Cybersecurity Resource Center <https://www.aicpa.org/cybersecurity>

Additional ? Questions

NFP Section

About the AICPA's NFP Section

- Get NFP tools and resources at your fingertips
- Receive exclusive discounts off the AICPA's NFP offerings, including events, publications, and products
- Find us at: www.aicpa.org/nfp
- Questions? Email us at NFPsection@aicpa.org.




NFP Section Benefits

- Subscription to eAlerts to keep you informed
- Four complimentary webcasts
- Access to resources in four key interest areas
 - Financial accounting and reporting
 - Assurance
 - Tax compliance
 - Governance and management

Fri 9/28/2018 11:33 AM
AN AICPA NFP Section <aicpanfp@e2.aicpa.org>
NFP Alert No. 2018-21, Implementing new accounting standards? We have you covered!

To Ashley Whitaker
Retention Policy 18 Months (w Recovery) (1 year, 6 months)
If there are problems with how this message is displayed, click here to view it in a web browser.

AICPA Not-for-Profit Section News and Events

 AICPA Not-for-Profit Section News
Helping those who serve others

September 28, 2018 — Volume 18 No. 21

Wednesday, October 24 — 2 CPE credits

Effective Board Policies
Produce Effective
Nonprofit Boards

A note to our members

We had a record-breaking turnout at our September webcast on implementing new accounting standards! Were you there? If you missed it, don't worry, it will be available in our [webcast archive](#) soon. In the meantime, don't forget you can find answers to lots of your questions and numerous actionable tools and resources to help you navigate these challenges in our [NFP Financial Reporting Resource Library](#).

FEATURED MEMBER BENEFITS

If you're implementing or preparing to implement new accounting standards, be sure to check out these and other resources:

[Revenue Recognition Implementation Is Upon Us](#)

[Conduit Debt Obligations: Is Your Not-for-Profit Scoped In or Out of Accelerated Effective Dates?](#)

[Leasing Activity by Not-for-Profit Entities Under FASB ASU 2016-02](#)

NFP Financial Reporting Standard: Top 5 Things Your Board Should Know ([Slides](#), archived [webcast](#): 9/13/17)

AICPA Staff

Chris Cole, CPA, CFE, CGMA
Associate Director

Ashley Whitaker, CPA
Lead Manager



Lana Richards, CPA
Manager

CPE Certificate

- As a reminder, you may access your CPE certificate by clicking the “Get CPE” icon if you have fulfilled the attendance check requirements.
- If you do not have an opportunity to obtain your CPE certificate during today’s presentation, you may obtain your certificate *after* 24 hours by logging back into the event and clicking the “Get CPE” icon. Please note that you will not be able to respond to the attendance checks in the archive, and you must fulfill the attendance requirements during the actual presentation to receive your CPE certificate.



Thank you

© 2019 Association of International Certified Professional Accountants. All rights reserved. This presentation's images are subject to copyright protection and used under license from third parties. No further use of images is permitted and use of copyrighted images outside the licensed scope constitutes copyright infringement and subjects the user to monetary damages and other penalties.