Training on Management Responsibilities under SAS 136 and DOL Cybersecurity Best Practices

CPAs & ADVISORS

Jennifer McCahill,
CPA
Partner, Audit
GRF CPAs & Advisors

Sarah Glynn,
CPA
Manager, Audit
GRF CPAs & Advisors

Mac Lillard,
CPA, CFE, CISA, CRISC, CITP
Manager, Risk & Advisory Services
GRF CPAs & Advisors

Housekeeping

CPE Credit/Technical Support

- **Important:** Three (3) CPE words will be provided during the presentation. Please write them down – **we will not provide them again via Zoom or email (no exceptions)**.
- Please complete the electronic survey that will appear automatically at the **end of the webinar**.
- Attendees seeking CPE for this presentation must complete the survey and **enter all three CPE words**. You cannot claim CPE unless we receive a completed evaluation with the correct words.
- This presentation will be recorded and made available to download at www.grfcpa.com/webinars.
- Technical questions about the survey can be addressed to Nathan McElveen at nmcelveen@grfcpa.com.

Housekeeping

Additional Information

Learning Objective To provide attendees with industry updates, guidance on 2021 changes and preparations for new accounting standards under SAS 136	**Instructional Delivery Methods** Group Internet-based
Recommended CPE 1.0 CPE Credit	**Recommended Fields of Study** Auditing – Technical
Prerequisites None required	**Advance Preparation** None
Program Level Basic	**Course Registration Requirements** None
Refund Policy No fee is required to participate in this session.	**Cancellation Policy** In the event that the presentation is cancelled or rescheduled, participants will be contacted immediately with details.
Complaint Resolution Policy GRF CPAs & Advisors is committed to our participants' 100% satisfaction and will make every reasonable effort to resolve complaints as quickly as possible. Please contact *k.davis@grfcpa.com* with any concerns.	
Disclaimer This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.	

Presenters

Meet the instructors

Jennifer McCahill, CPA

Partner, Audit

Mac Lillard, CPA, CFE, CISA, CRISC, CITP

Manager, Risk & Advisory Services

Sarah Glynn, CPA

Manager, Audit

INSIDE PUBLIC ACCOUNTING TOP 200 FIRMS 2021

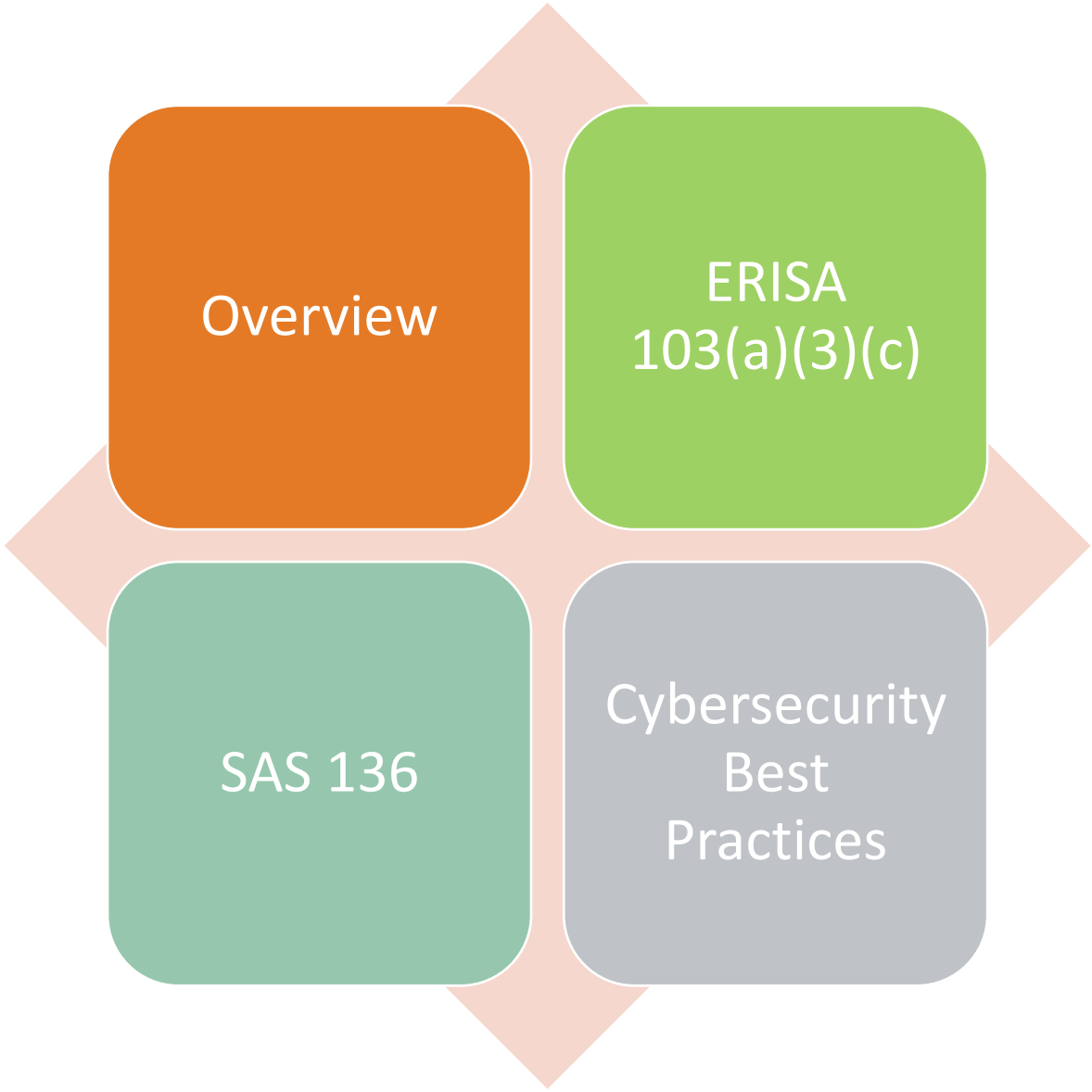
ACCOUNTINGTODAY 2022 Regional Leaders

ACCOUNTINGTODAY 2021 Best Firms to Work For

ACCOUNTINGTODAY 2022 Firms to Watch

grf CPAs & ADVISORS

Agenda


Overview
ERISA 103(a)(3)(c)
SAS 136
Cybersecurity Best Practices

Training

SAS 136 – Implemented for 2021 Plan Year Ends

grf CPAs & ADVISORS

Polling Question #1

Are you aware of the changes to "limited scope" audits under SAS 136?

A. Yes

B. No

C. Unsure

grf CPAs & ADVISORS

Understand Employee Benefit Plan Audits

SAS No. 136 Highlights

Limited Scope Audit (ERISA Section 103(a)(3)(c) Audit)

Create a different audit opinion (language) when plan management/sponsor engages a firm to perform a "limited scope" audit

Additional Work on Certifications

Additional audit procedures will have to be applied to investment certifications

Audit Opinion on Compliance

The auditor will have to report on specific plan provisions and whether or not the Plan has complied

Understand Employee Benefit Plan Audits

Changes Under SAS No. 136

Clarify and expand on Plan Sponsor responsibilities	- Assess whether the certifying institution is qualified - Certified investment information is appropriately measured, presented and disclosed in accordance with the applicable financial reporting framework. - Maintaining a current plan document and amendments, etc. - Maintain sufficient participant records
Clarify and expand on the Auditor's responsibilities	- Communicate "reportable findings" - Review draft of Form 5500 prior to finalization

Employee Benefit Plan Update

SAS No. 136

DO ANY OF THE CHANGES AFFECT PLAN MANAGEMENT (SPONSOR/ADMINISTRATOR?)

1. **As part of the auditor's acceptance of the engagement the auditor will ask plan management to acknowledge the responsibilities for maintaining the plan, administering the plan and providing a draft 5500**

2. **Most Significant Change: Requires the auditor to obtain from plan management (in writing) representation that management:**
   - Elects to have an ERISA Section 103(a)(3)(c) audit
   - Whether that audit is permissible
   - The investment information is prepared and certified by a qualified institution
   - The Certification meets DOL requirements
   - The certified information is appropriately measured, presented and disclosed in accordance with the applicable framework.

Employee Benefit Plan Update

SAS No. 136

Explore the Management

Certification Assessment Tool

PDF Available on GRF website event page

EXAMPLE 1

Principal Certification Example

PDF Available on GRF website event page

EXAMPLE 2

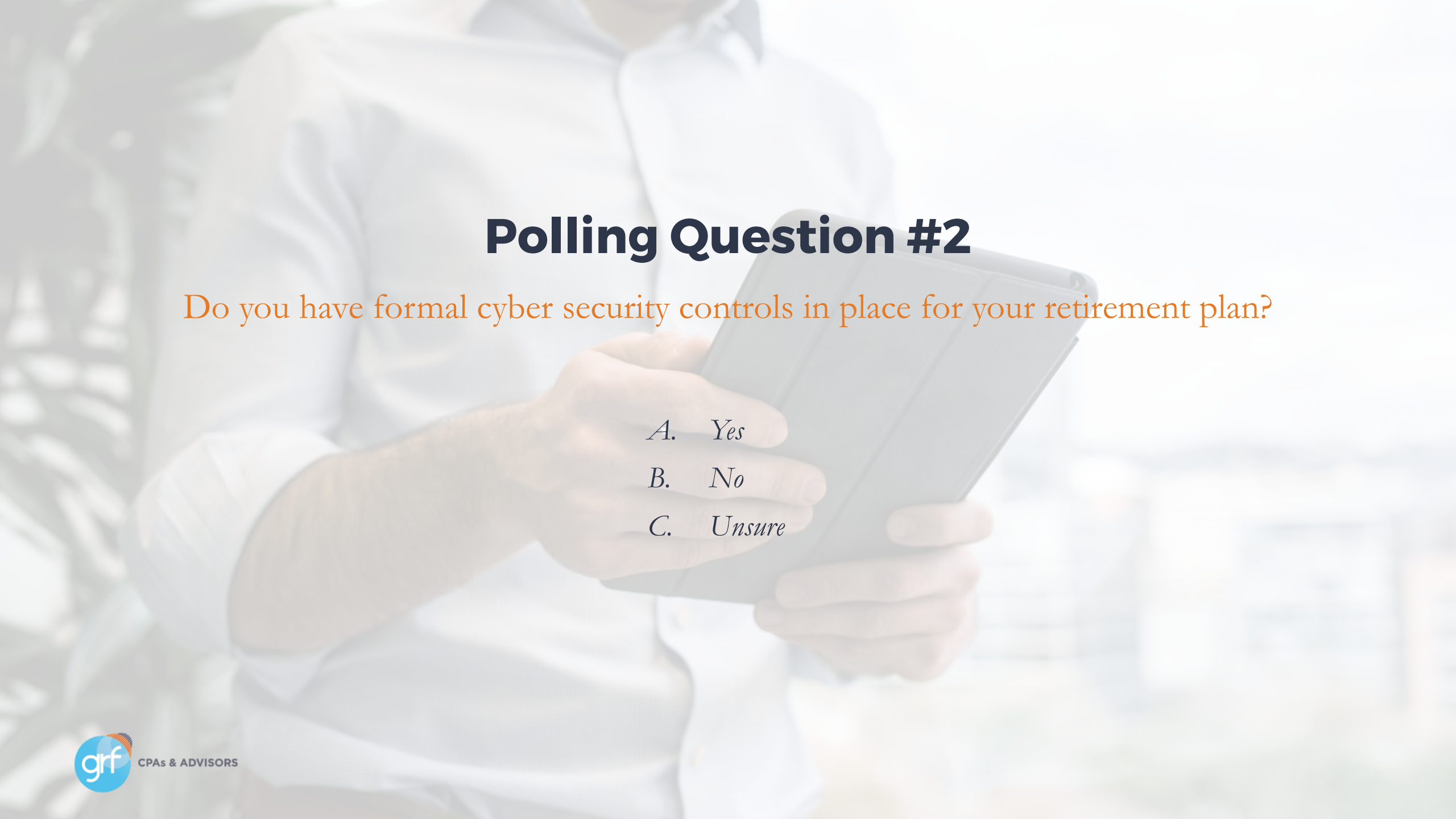
Trustee Certification Example

PDF Available on GRF website event page

Employee Benefit Plan

DOL's Cybersecurity Best Practices

grf CPAs & ADVISORS



Polling Question #2

Do you have formal cyber security controls in place for your retirement plan?

A. Yes

B. No

C. Unsure

grf CPAs & ADVISORS

DOL Cyber Security Background

DOL's view on Cyber Security for Plans

The DOL and EBSA are currently in the process of conducting a study on **Cyber Security** related to retirement plans and what procedures service providers and plan administrators have in place.

Currently, there is no formal guidance on what the DOL and EBSA would expect as far as a minimum requirement for **Cyber Security controls**. They will most likely issue formal guidance upon conclusion of their research.

DOL Cyber Security Background

DOL's view on Cyber Security for Plans

- Management/Plan Administrators are responsible for ensuring compliance with the plan
- Management/Plan administrators are responsible for the administration of the plan, **even** if outsourced to a third party institution. The onus falls on the employer. And this includes establishing internal controls around cyber and data security or ensuring that the service provider has good controls in place.
- DOL has issued the following guidance (via link here) to what they consider best practices for a Plan's Cyber Security.

DOL Cyber Security Background

DOL's view on Cyber Security for Plans

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

Cybersecurity Best Practices for Retirement Plans

Overview

- DOL Best Practices
- Understanding your organization's context and custom-tailoring your cybersecurity program
- Understanding the roles of management versus roles of outside parties

Cybersecurity Best Practices for Retirement Plans

Policies and Procedures

- 1. Have a formal, well documented cybersecurity program
  - Formally developed policies and procedures for the organization
  - Addresses all cyber controls implemented by an outside party or by the organization
- 4. Clearly define and assign Information Security roles and responsibilities
  - Accountability for all employees (not just IT professionals)
- 5. Have strong access control procedures
  - Periodic review of access rights
- 7. Conduct periodic cybersecurity awareness training
  - Onboarding, annually, ongoing phishing simulations
- 8. Implement and manage a secure system development life cycle (SDLC) program
  - Identify ways to automate, optimize, and continuously improve upon the existing infrastructure and practices
- 10. Encrypt sensitive data stored and in transit
  - Define risk classification methodology and assign to data
- 11. Implement strong technical controls in accordance with best security practices

Cybersecurity Best Practices for Retirement Plans

Risk Management

- 2. Conduct prudent annual risk assessments
  - Identify deficiencies for remediation
  - Identify areas for improvement/automation/optimization
- 3. Have a reliable annual third-party audit of security controls
  - Independent cybersecurity assessment
- 6. Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments
  - Review of SOC II Reports
  - Financial viability and other items

Cybersecurity Best Practices for Retirement Plans

Business Resiliency and Incident Response

- 9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
  - Clearly defined roles and responsibilities
  - Tabletop scenarios
  - Log of incidents, response time, business impact, root-cause
- 12. Appropriately respond to any past cybersecurity incidents
  - After Action Report
  - Root-cause and business impact analysis

Communicating IT Items to the Board

Education, Monitoring, and Reporting

Education:

- SAS 145 and Auditor Comments
- High-level overview of processes implemented by management

Monitoring and Reporting

- Leverage existing meetings
- Set as a recurring agenda item
- Top Risks and Mitigation Plans
- Avoid getting too granular
- Break it down in simple terms (avoid technical jargon)
- Dashboards

grf CPAs & ADVISORS

Polling Question #3

Did you learn a few key take-aways to bring back to your own organization?

A. Yes

B. No

C. Unsure

grf CPAs & ADVISORS

Questions?

Contact Us

CPAs & ADVISORS

DC | New York

877-437-4771 | www.grfcpa.com

Jennifer McCahill, CPA
Partner, Audit
jmccahill@grfcpa.com

Mac Lillard, CPA, CFE, CISA, CRISC, CITP
Manager, Risk & Advisory Services
mlillard@grfcpa.com

Sarah Glynn, CPA
Manager, Audit
sglynn@grfcpa.com

Disclaimer

This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. While we use reasonable efforts to furnish accurate and up-to-date information, we do not warrant that any information contained in or made available in this presentation is accurate, complete, reliable, current or error-free. We assume no liability or responsibility for any errors or omissions in the content of this presentation.

The use of the information provided in this presentation does not establish any contractual or other form of client engagement between GRF CPAs & Advisors and the reader or user. Any U.S. federal tax advice contained in this presentation is not intended to be used for the purpose of avoiding penalties under U.S. federal tax law. Readers and users of this presentation information are advised not to act upon this information without seeking the service of a professional accountant.