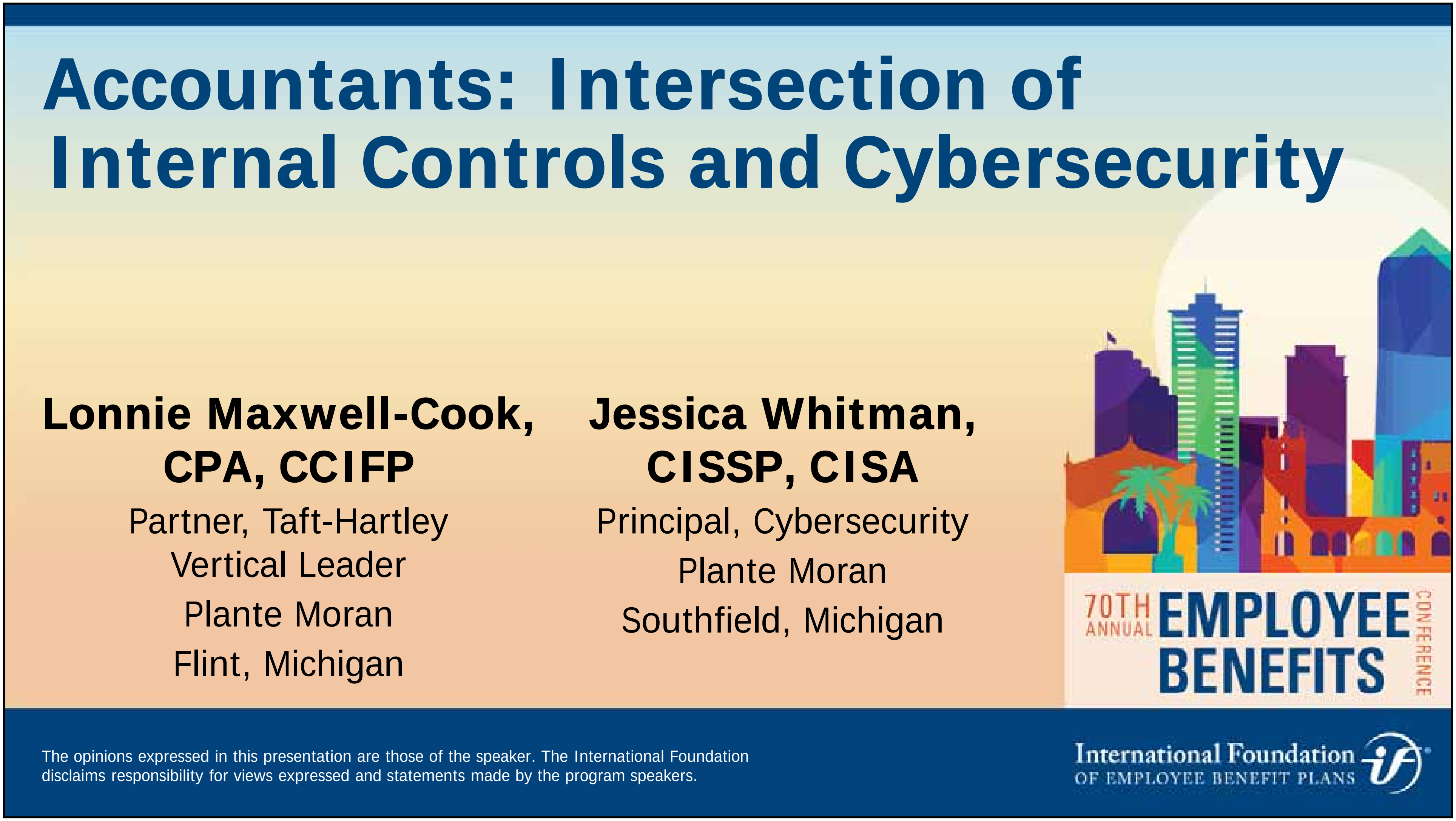


# Accountants: Intersection of Internal Controls and Cybersecurity

**Lonnie Maxwell-Cook, CPA, CCIFP**

Partner, Taft-Hartley Vertical Leader

Plante Moran

Flint, Michigan

**Jessica Whitman, CISSP, CISA**

Principal, Cybersecurity

Plante Moran

Southfield, Michigan

70TH ANNUAL EMPLOYEE BENEFITS CONFERENCE

The opinions expressed in this presentation are those of the speaker. The International Foundation disclaims responsibility for views expressed and statements made by the program speakers.

International Foundation OF EMPLOYEE BENEFIT PLANS

# Session Overview

- Penetration testing
- Third party security controls
- Documentation
- What is being found?

# But First, What Is the Current Cyber Environment?

**Let's start here:**

- Hackers: Stronger than ever
- Reasons: Ever-expanding
- Business Perception: Security = IT
- Problem: Resources (supply) < Demand
- Incidents: Not if, but when
- Cost of a Breach: Rising (dramatically)
- Clients: Expect security
- Legal/Regulatory: You are guilty until proven otherwise
- Perception: No one will target me

# Recent Incidents

72%

of businesses worldwide were affected by ransomware as of 2023.
Source: Statista

8 out of 10

Organizations had at least one individual who fell victim to a phishing attempt by CISA Assessment teams.
Source: CISA

# What Is the Current Cyber Environment?

**Valid accounts and phishing are now tied** as the top initial access vectors. Obtaining valid credentials is easier for attackers to obtain their goals.

**Data Theft/Leakage** is the new #1 incident impact making up for 32% of incidents. **Extortion** and **Credential Harvesting** are also common impacts of incidents.

Increase in cyber attacks on **small and mid-sized businesses** due to large businesses investing heavily in cybersecurity

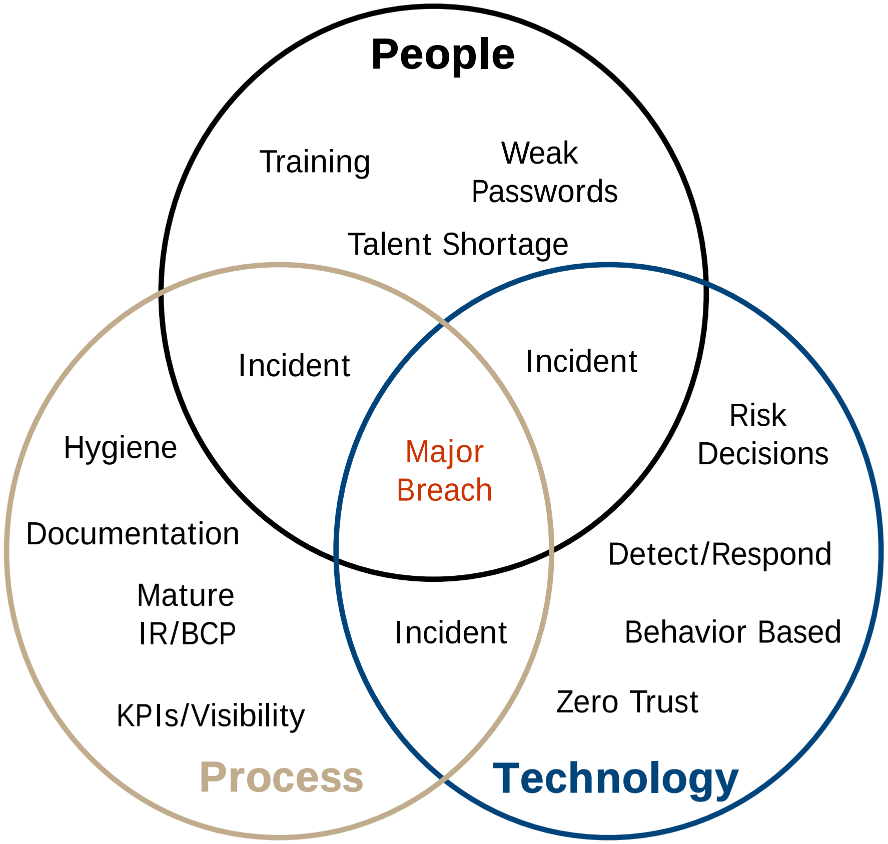
Increase in **malware infections** spread by USB devices, PDF files, IoT devices, and malicious mobile apps.

**Generative AI** is currently being explored by cybercriminals to aid in cyber attacks. Expect to see increase in AI-enabled attacks as AI tools mature.

**93%** of CISOs expect an increase in their cybersecurity budget over the next year, yet 83% see cuts in other departments, showing the prioritization of IT Security.

**Data privacy regulations** continue to drive change in the cybersecurity landscape

# Why Are Organizations Vulnerable?



# Penetration Testing

# What Is Penetration Testing?

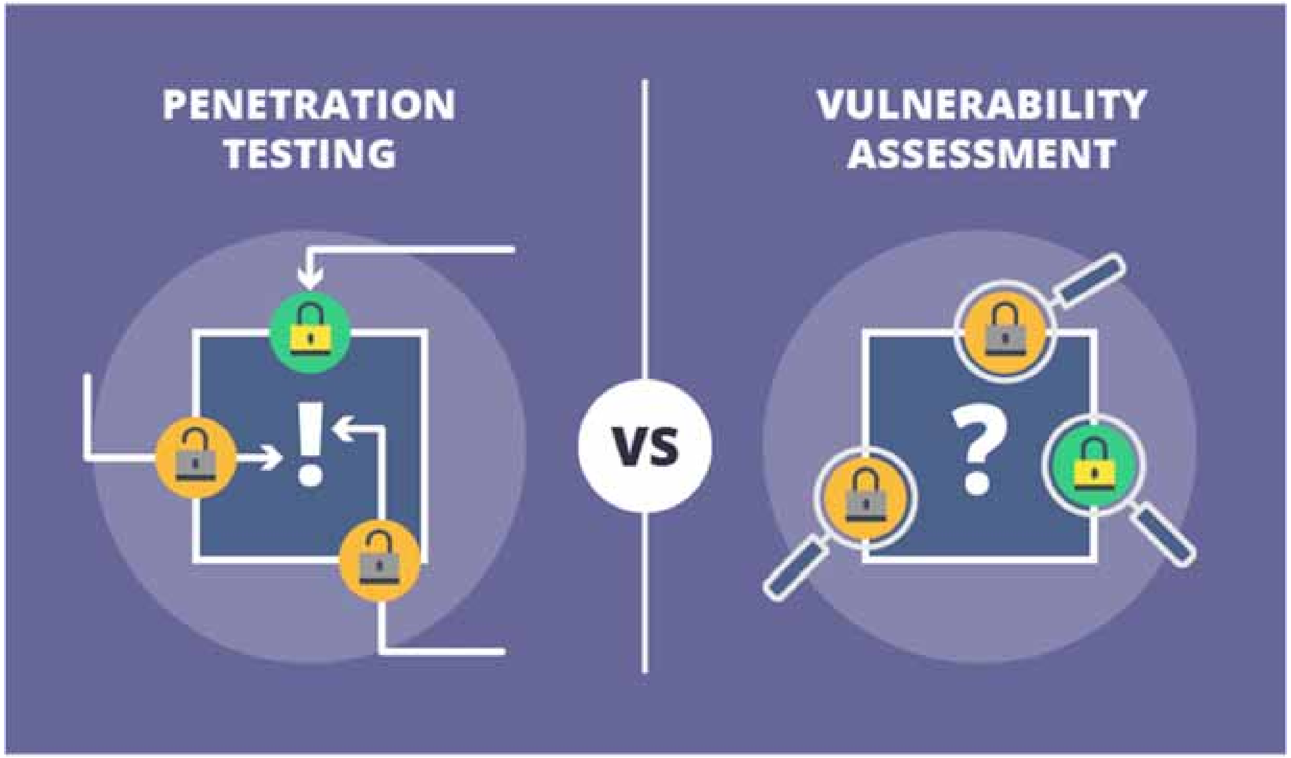
“**Penetration testing** is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. … All parties agree to the rules of engagement before the commencement of **penetration testing** scenarios.”

– NIST 800-53

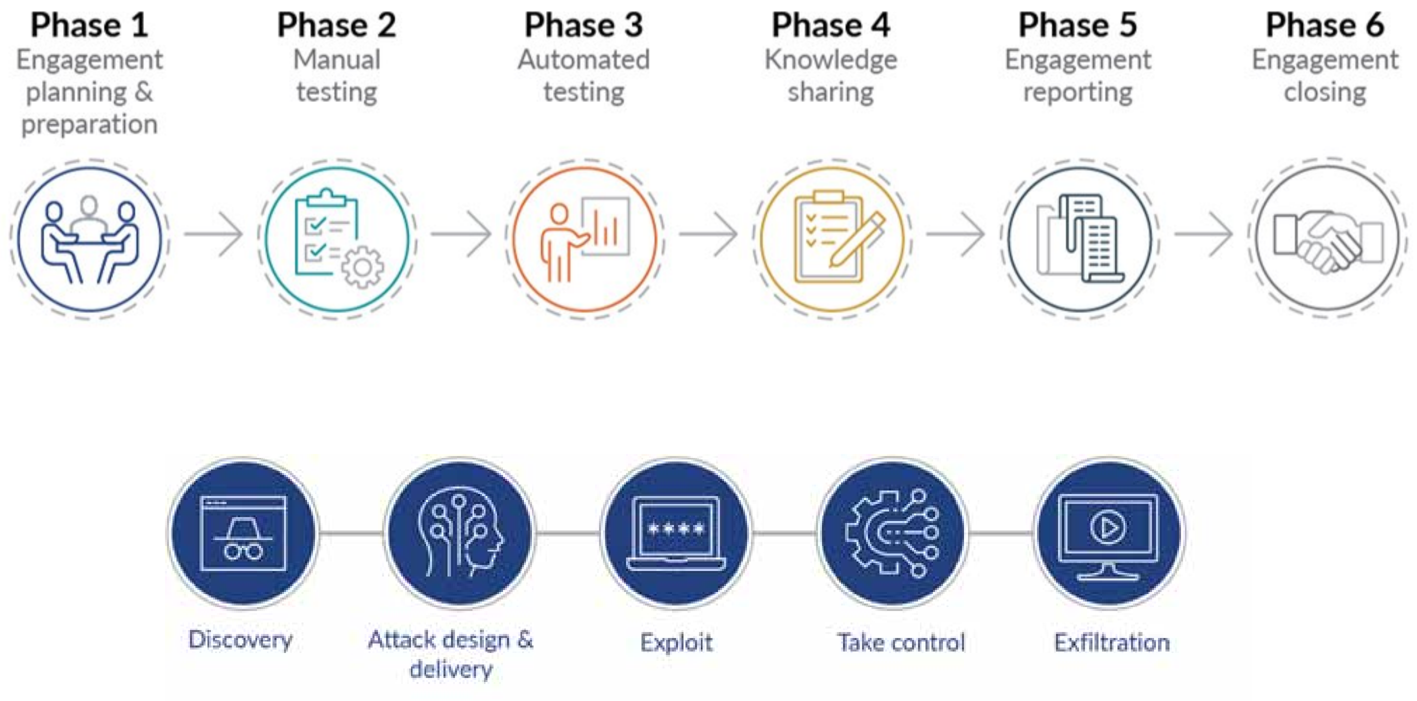
# Penetration Testing vs. Hacking

- Ethical hacking
- Agreements
  - Defined scope
  - Pre-determined length of time
  - Point of contact, shared contact information
  - Stipulations on what you can and cannot do
- Third-party systems

# Penetration Testing vs. Vulnerability Scan



# Pen Testing Methodology

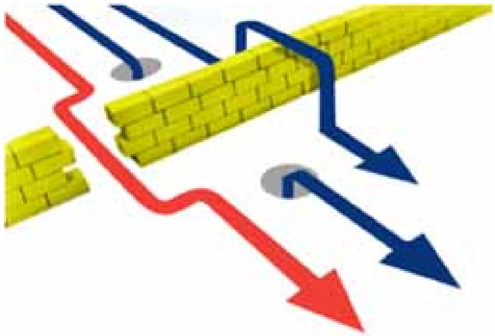


# Type of Penetration Tests

- Network
- Wireless
- Web App
- Mobile App
- IoT
- Social Engineering
- Red team/Blue Team exercise

# Why Are Penetration Tests Important?

- Test existing security controls
- Discover weaknesses
- Compliance requirements
- Understand detective capabilities
- Areas to invest in security
- Outside perspective
- Save money

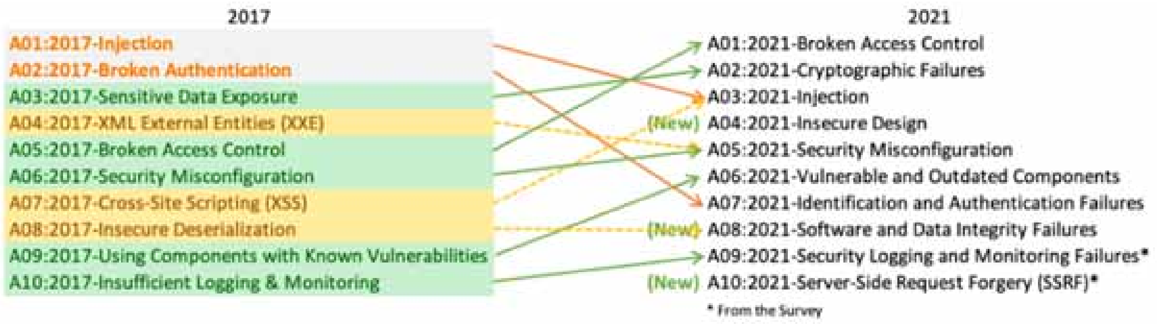


# Pen Testing Risks and Concerns

- Type of pen test (more likely a vulnerability scan)
- Unqualified pen testers
- No methodology or framework followed
- Not addressing your main concerns/areas of risk
- Don’t understand your line of business

# Pen Testing Recommendations

- Find a good pen tester (referrals, skills)
- Methodology is important
- Follows a framework
- Qualifications and experience
- Understand your goals/outcomes of pen test



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

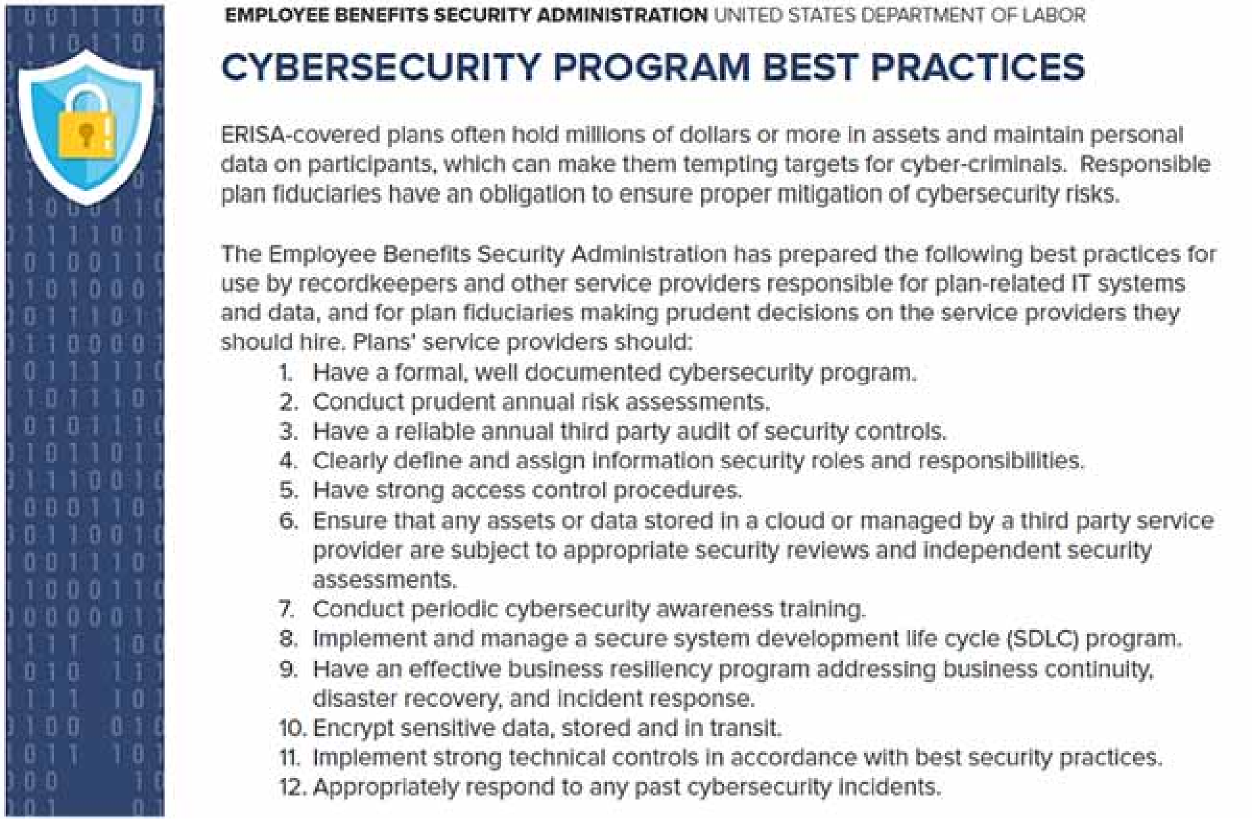
2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

# Third-Party
# Security Controls

# Department of Labor Best Practices



**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.

Source: US Department of Labor

# DOL #1-3

1. Formal well-documented cybersecurity program
   - Adopt a control framework
   - Maintain and monitor controls
2. Conduct annual risk assessments
3. Have a reliable 3rd party audit of security controls.

# DOL #4-6

4. Clearly define and assign info sec. roles and responsibilities (information security policies)
5. Have strong access control procedures
6. Ensure assets/data stored in cloud are subject to appropriate security reviews (vendor management)

## DOL #7-9

7. Conduct periodic security awareness training.
8. Implement and manage a secure system development life cycle program (change management)
9. Business continuity, disaster recovery, and incident response

# DOL #10-12

10. Encrypt sensitive data—Stored and in transit.
11. Implement strong technical controls.
12. Appropriately respond to past cybersecurity incidents.

# Documentation—
# How It's Used in the Audit and
# How to Understand the Audit Report

# Ready for Some Fun

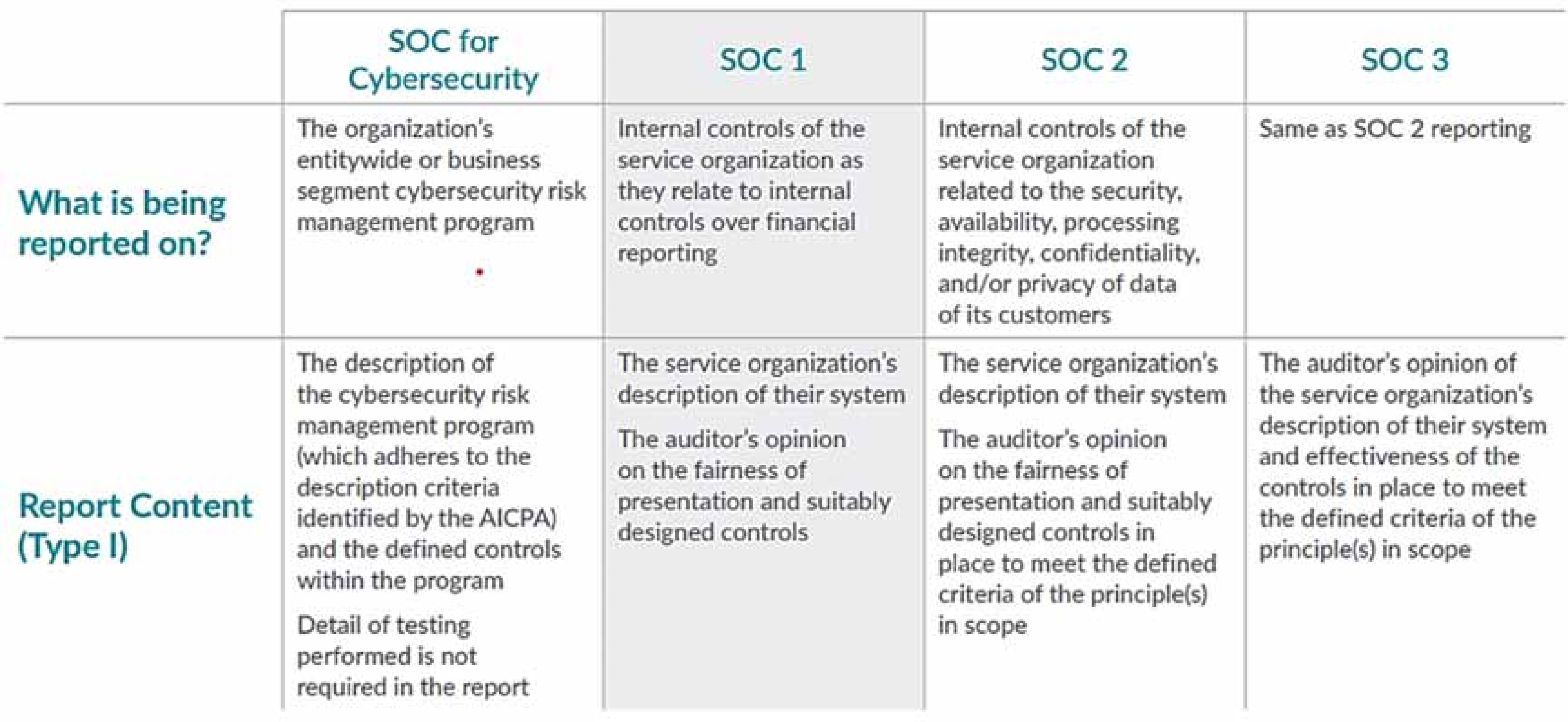
## DOL and Cybersecurity

- Prime targets for cyber attacks
- 140 million participants in ERISA-governed plans
- Assets of $9.3 trillion
- Maintain significant amounts of sensitive data

# Document, Document, Document

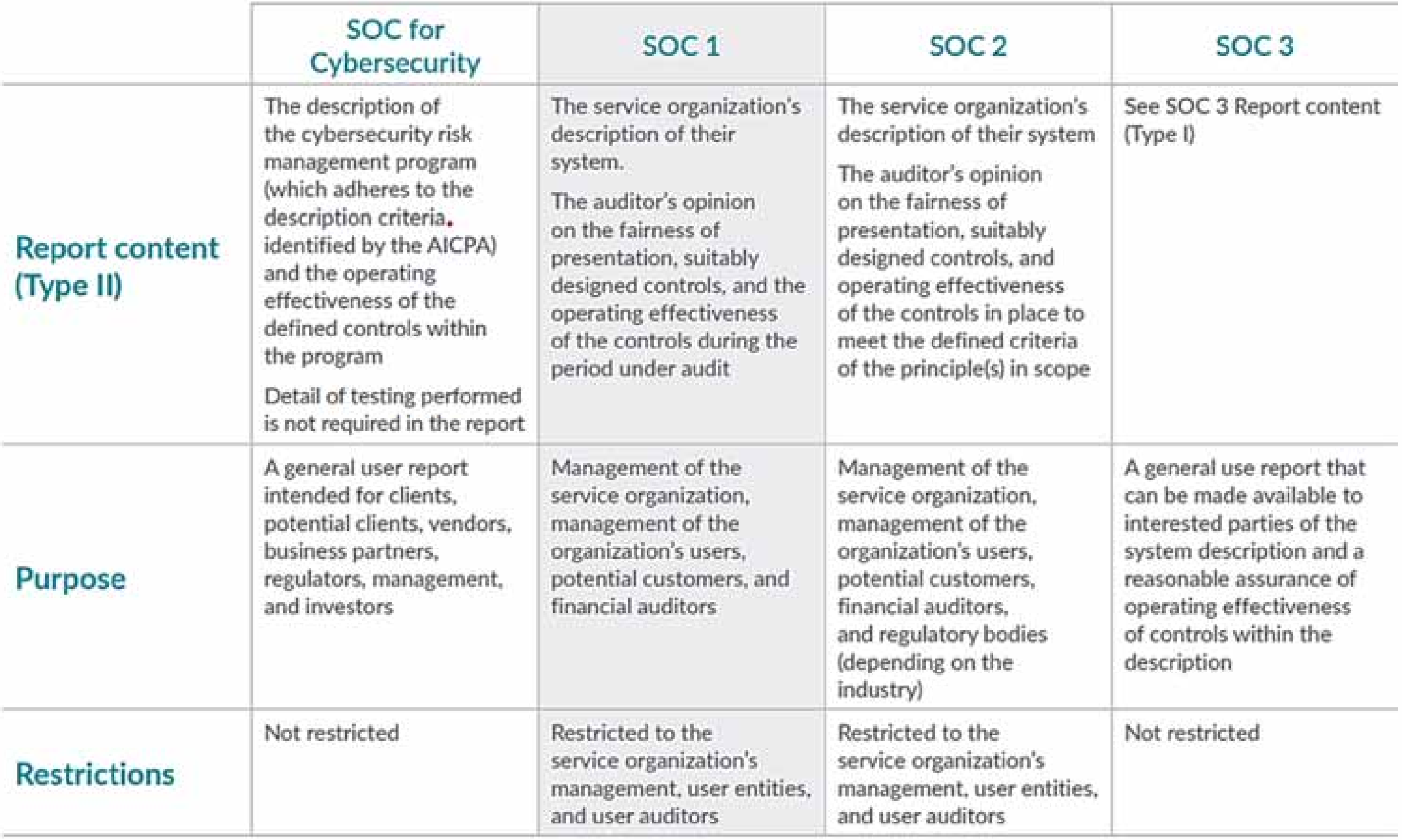
- Assess how controls of the IT environment can impact the financial statement audit
  - Do they have cybersecurity policies and procedures
  - Who has access to server rooms?
  - Password policies
  - Process of controlling data
  - Assessment of service providers controlling data

# SOC Suite



| | SOC for Cybersecurity | SOC 1 | SOC 2 | SOC 3 |
|---|---|---|---|---|
| What is being reported on? | The organization's entitywide or business segment cybersecurity risk management program | Internal controls of the service organization as they relate to internal controls over financial reporting | Internal controls of the service organization related to the security, availability, processing integrity, confidentiality, and/or privacy of data of its customers | Same as SOC 2 reporting |
| Report Content (Type I) | The description of the cybersecurity risk management program (which adheres to the description criteria identified by the AICPA) and the defined controls within the program<br>Detail of testing performed is not required in the report | The service organization's description of their system<br>The auditor's opinion on the fairness of presentation and suitably designed controls | The service organization's description of their system<br>The auditor's opinion on the fairness of presentation and suitably designed controls in place to meet the defined criteria of the principle(s) in scope | The auditor's opinion of the service organization's description of their system and effectiveness of the controls in place to meet the defined criteria of the principle(s) in scope |

# SOC Suite



| | SOC for Cybersecurity | SOC 1 | SOC 2 | SOC 3 |
|---|---|---|---|---|
| Report content (Type II) | The description of the cybersecurity risk management program (which adheres to the description criteria. identified by the AICPA) and the operating effectiveness of the defined controls within the program<br>Detail of testing performed is not required in the report | The service organization's description of their system.<br>The auditor's opinion on the fairness of presentation, suitably designed controls, and the operating effectiveness of the controls during the period under audit | The service organization's description of their system<br>The auditor's opinion on the fairness of presentation, suitably designed controls, and operating effectiveness of the controls in place to meet the defined criteria of the principle(s) in scope | See SOC 3 Report content (Type I) |
| Purpose | A general user report intended for clients, potential clients, vendors, business partners, regulators, management, and investors | Management of the service organization, management of the organization's users, potential customers, and financial auditors | Management of the service organization, management of the organization's users, potential customers, financial auditors, and regulatory bodies (depending on the industry) | A general use report that can be made available to interested parties of the system description and a reasonable assurance of operating effectiveness of controls within the description |
| Restrictions | Not restricted | Restricted to the service organization's management, user entities, and user auditors | Restricted to the service organization's management, user entities, and user auditors | Not restricted |

# Statement of Auditing Standards 145

- SAS 145
  - Boarder strategic objective to converge International Standards on Auditing (ISA)
  - Enhances requirements and guidance on auditor's risk assessment (enhance audit quality)
  - Address risk arising from use of IT environment and controls
  - Effective for audits on or after December 15, 2023 (*i.e.*, December 31, 2023 audits)

# Statement of Auditing Standards 145

- SAS 145 *(continued)*
  - Key concepts are not fundamentally changing
  - Requirement to assess control risk at maximum if not testing controls for operating effectiveness
    - Audit risk (AR) = Inherent Risk (IR) x Control Risk (CR) x Detection Risk (DR)
    - The higher the control risk, the lower the detection risk must be.
    - This may require more substantive audit work (larger sample sizes)

# Statement of Auditing Standards 145

- SAS 145 *(continued)*
  - More focused assessment to identify and perform deeper evaluation of the controls (identified controls)
  - New “Stand-Back”, drive an evaluation of completeness of auditor’s identification of significant classes of transactions, account balances and disclosures
  - New guidance related to maintaining professional skepticism

# Statement of Auditing Standards 145

- SAS 145 *(continued)*
  - Communicate to those charged with governance
  - Additional testing necessary
  - Costs should be considered in current year fee structure
  - See SAS 145 Appendix F—Considerations for Understanding General IT Controls

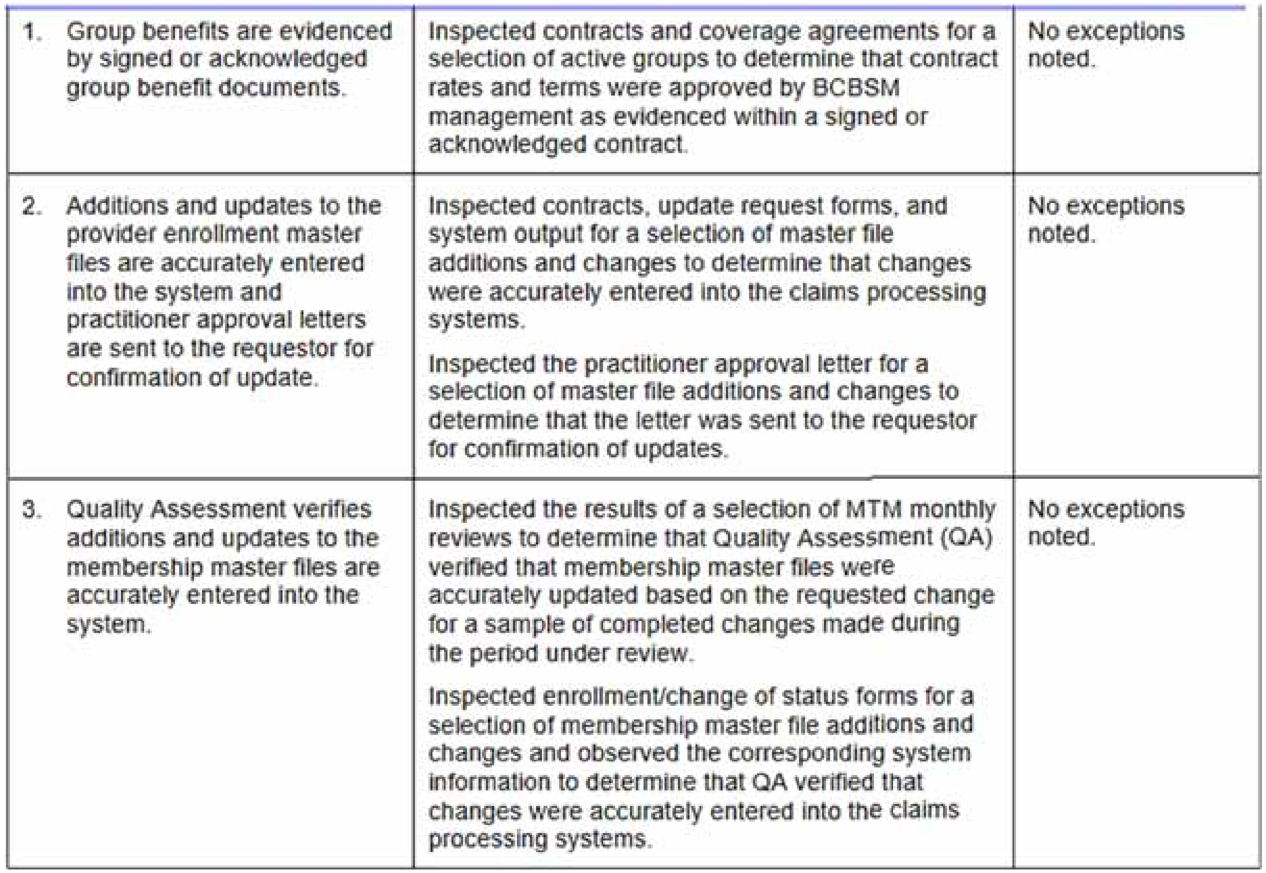
# Internal Control Monitoring

- The internal controls in place for cybersecurity should be monitored regularly
- The individuals responsible for enforcing controls should be the ones to create/maintain cyber program

# Document, Document, Document

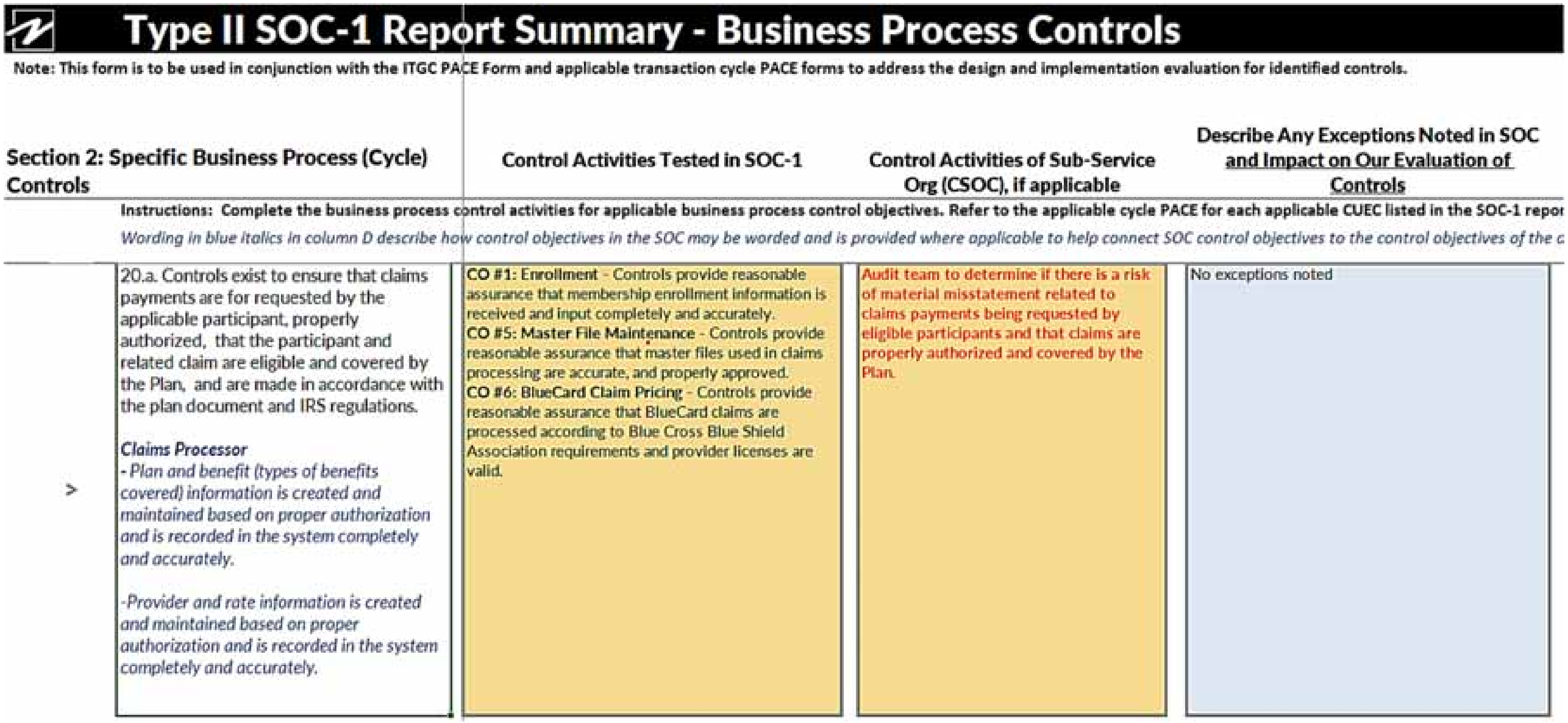
- Simply obtaining the SOC 1 report and placing it in the audit workpapers does not satisfy the requirements of Generally Accepted Auditing Standards (GAAS)
- Need to review SOC 1 report, and document findings or issues that could impact matters effecting the financial statement environment

# Document, Document, Document



| | | |
|---|---|---|
| 1. Group benefits are evidenced by signed or acknowledged group benefit documents. | Inspected contracts and coverage agreements for a selection of active groups to determine that contract rates and terms were approved by BCBSM management as evidenced within a signed or acknowledged contract. | No exceptions noted. |
| 2. Additions and updates to the provider enrollment master files are accurately entered into the system and practitioner approval letters are sent to the requestor for confirmation of update. | Inspected contracts, update request forms, and system output for a selection of master file additions and changes to determine that changes were accurately entered into the claims processing systems.<br>Inspected the practitioner approval letter for a selection of master file additions and changes to determine that the letter was sent to the requestor for confirmation of updates. | No exceptions noted. |
| 3. Quality Assessment verifies additions and updates to the membership master files are accurately entered into the system. | Inspected the results of a selection of MTM monthly reviews to determine that Quality Assessment (QA) verified that membership master files were accurately updated based on the requested change for a sample of completed changes made during the period under review.<br>Inspected enrollment/change of status forms for a selection of membership master file additions and changes and observed the corresponding system information to determine that QA verified that changes were accurately entered into the claims processing systems. | No exceptions noted. |

# Document, Document, Document



## Type II SOC-1 Report Summary - Business Process Controls

Note: This form is to be used in conjunction with the ITGC PACE Form and applicable transaction cycle PACE forms to address the design and implementation evaluation for identified controls.

**Instructions:** Complete the business process control activities for applicable business process control objectives. Refer to the applicable cycle PACE for each applicable CUEC listed in the SOC-1 repor

*Wording in blue italics in column D describe how control objectives in the SOC may be worded and is provided where applicable to help connect SOC control objectives to the control objectives of the c*

| Section 2: Specific Business Process (Cycle) Controls | | Control Activities Tested in SOC-1 | Control Activities of Sub-Service Org (CSOC), if applicable | Describe Any Exceptions Noted in SOC and Impact on Our Evaluation of Controls |
|---|---|---|---|---|
| > | 20.a. Controls exist to ensure that claims payments are for requested by the applicable participant, properly authorized, that the participant and related claim are eligible and covered by the Plan, and are made in accordance with the plan document and IRS regulations.<br>*Claims Processor*<br>*- Plan and benefit (types of benefits covered) information is created and maintained based on proper authorization and is recorded in the system completely and accurately.*<br>*-Provider and rate information is created and maintained based on proper authorization and is recorded in the system completely and accurately.* | **CO #1: Enrollment** - Controls provide reasonable assurance that membership enrollment information is received and input completely and accurately.<br>**CO #5: Master File Maintenance** - Controls provide reasonable assurance that master files used in claims processing are accurate, and properly approved.<br>**CO #6: BlueCard Claim Pricing** - Controls provide reasonable assurance that BlueCard claims are processed according to Blue Cross Blue Shield Association requirements and provider licenses are valid. | Audit team to determine if there is a risk of material misstatement related to claims payments being requested by eligible participants and that claims are properly authorized and covered by the Plan. | No exceptions noted |

# Document, Document, Document

- Assess whether these are reviewed internally by TPA or self-administered finance teams
- Communicate to those charged with governance if no review by internal finance teams

# What Is Being Found?

# Overview of Common Findings

- Pen test findings
- Access
- Vendors
- Asset inventory
- Asset management
- Change management

# Common Pen Test Findings

- Weak passwords
- Default credentials
- Shared passwords

# Common Cybersecurity Findings

- Unauthorized Access
  - Elevated permissions
  - Access not granted using “least privilege”
  - Poor segregation of duties
  - Terminated users with lingering access

What are the risks associated?

# Considerations for Access

- How are employment changes communicated?
- Who has access to what?
- Are user access reviews performed?
  If so, what is the process?

# Common Findings—Access

- Elevated permissions
  - Users may have administrative access that is not needed, or have access to folders, systems, or applications that are unnecessary

REMEDIATION:

- User access review (annually minimum)
- Concept of least privilege application
- Activity may be unmonitored, logged but not reviewed, etc.—Define actions that require review

# Common Findings—Access

- Poor segregation of duties
  - Users may have conflicting access
    - Code development
    - Financial application access permissions

REMEDIATION:

- Segregate duties where possible
- Implement reviews/alerting

# Common Findings—Access

- Terminated users with lingering access
  - Users who have been terminated may still have active accounts to applications
  - Key card/badge not returned, disabled

REMEDIATION:

- Implement access policy and procedure
- Automate termination processes

# Common Cybersecurity Findings

- Vendor management
  - Vendor onboarding
  - Vendor contracts
  - Vendor management/annual review

What are the risks associated?

# Common Findings—Vendors

- Vendor onboarding
  - Vendors are hired without vetting process
  - Contracts do not contain security requirements, no recourse for issues

REMEDIATION:

- Vendor onboarding policy/procedure
- Vendor contractual requirements/contract reviews

# Common Findings—Vendors

- Vendor management
  - Management may not be aware of all vendors with access to systems
  - Understand high risk vendor access
  - Review and oversee vendors

REMEDIATION:

- Vendor management system/program
  - Third-party risk management

# Common Findings—Asset Inventory

- Assets are not inventoried/tracked
- Assets are unprotected
- Lost/stolen without knowledge
- Not aware of what devices are accessing network
- Shadow IT

REMEDIATION:

- Asset inventory solution
- Network scanning

# Common Findings—
# Workstation and Server Security

- Security agents not being fully deployed
- Devices unmonitored
- Devices not being patched
  - Problem comes back to losing visibility into devices

REMEDIATION:

- Asset inventory/visibility
- Patch management
- Antivirus management

# Common Findings—Change Management

- What stops unauthorized changes from being implemented?
- Overreliance on segregation of duties
- Change logs can be very difficult to make sense of

REMEDIATION:

- Change deployment alerting
- Review and approval process
- SDLC

# Key Takeaways

- Pen testing—A great way to understand your environment’s vulnerabilities, and validate security controls
- Third party security controls are important to understand and review
- Documentation is necessary for audits to be in compliance with GAAS
- Understand how to remediate common findings

**Your Feedback Is Important. Please Scan This QR Code.**

Session Evaluation