



*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

# Higher Education Virtual Conference

## 2025 and Beyond: Higher Education Trends and Insights from Industry Leaders

February 25, 2025



The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

# CPE Qualifications

To qualify for the full **4 CPE credits**, the following requirements must be met:



**Attend 200 minutes** of this session



**16 attendance markers** will be sent (*8 will be statements reading "I'm here" and 8 will be Qualifying Questions*).

You must **respond to a minimum of 12** out of those 16 attendance markers



# Agenda:

- *Intro*
- Regulatory Roadmap: Navigating Higher Ed Compliance
- *Break*
- Future-Ready: Generational Diversity and Hybrid Work
- *Break*
- Game On: Understanding the NIL and NCAA Reforms
- *Break*
- Ethical Hacking: A Primer on Penetration Testing for Non-IT Professionals
- *Closing*





# Regulatory Roadmap

Navigating Higher Ed Compliance



# Learning Objectives

---

Recognize the latest regulations affecting higher education

---

List recommended practices in supporting and implementing the latest regulations



How effective has your institution been at addressing regulatory changes and new standards?

- a) *Very effective*
- b) *Somewhat effective*
- c) *We are not making progress, but we should be able to handle it on our own*
- d) *We are not making progress, and I'd like CLA to contact me to discuss how they can help*





# Uniform Grant Guidance



©2025 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAglobal.com/disclaimer](https://www.claglobal.com/disclaimer). Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



# Uniform Grant Guidance

## OMB's objectives

Incorporate  
statutory  
requirements  
and  
administrative  
priorities

Reduce agency  
and recipient  
burden

Add clarity to  
sections that  
have been  
interpreted  
differently

Using plain  
language and  
addressing  
inconsistent use  
of terms



Final rules were issued in April 2024 , effective 10/1/24



# Uniform Grant Guidance – *Changes*

Increase single audit  
threshold from  
\$750,000 to \$1,000,000

Type A  
threshold increased to  
\$1,000,000

Modify the  
definition of  
questioned costs



# Uniform Grant Guidance – *Changes*

*Amount, expended or received from a Federal award in the auditor's judgement*

1. is **noncompliant or suspected noncompliant** with federal statues, regulations, or the terms and conditions of the federal award
2. at the time of the audit **lacked adequate documentation** to support compliance or
3. appeared **unreasonable** and **did not reflect the actuations** a prudent person would take in the circumstances`



# Uniform Grant Guidance – *Changes continued*



## Fixed amount subawards

- Previously capped at \$250,000; increased to \$500,000, federal agency approval still required



## Schedule of Federal Expenditures

- Proposed changes to disaggregate the SEFA did **NOT** make the final version!

# Uniform Grant Guidance – *Changes continued*

Term non-federal replaced with recipient or subrecipient throughout subparts

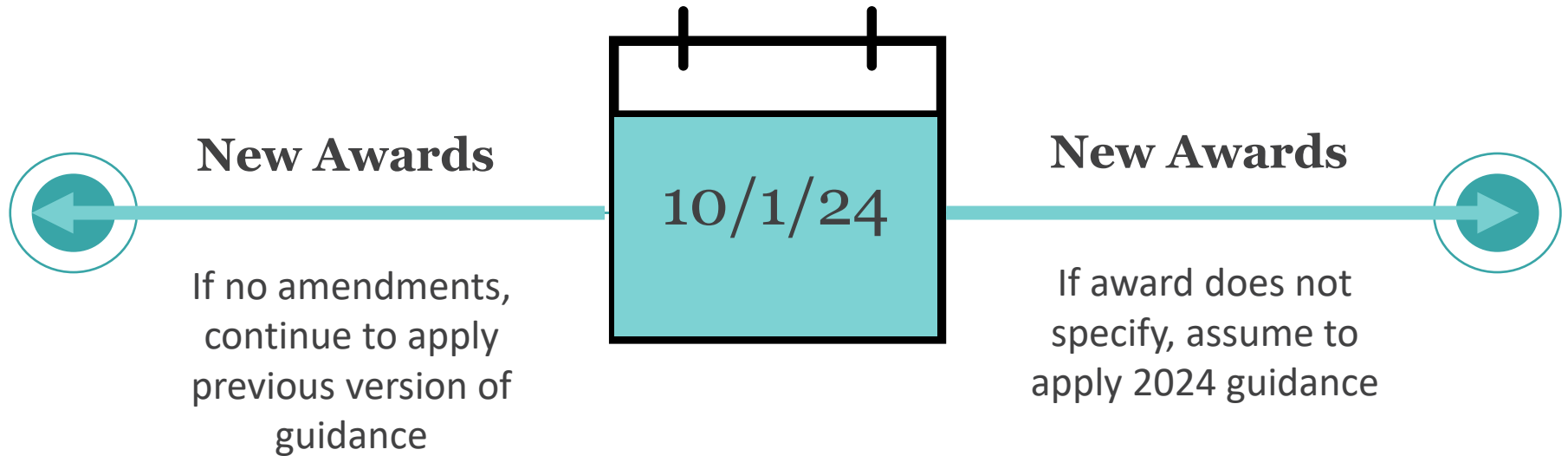
Increased de minimus indirect cost rate percentage from 10% to 15%

Threshold used to define a capital expenditure increased from \$5,000 to \$10,000

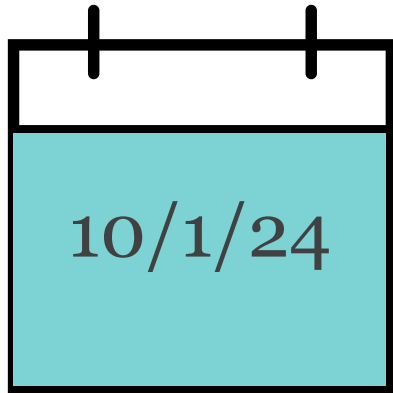
Section 200.407, 9 items removed from requiring prior approval (Real property, equipment, entertainment...)



# General Implementation Provisions



# General Implementation Provisions



## Amendments

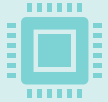
Assume to continue guidance from original award, but Federal agencies "strongly encouraged" to apply 2024 Revisions to additional funds

## Subawards

If Federal agency has amended, must amend existing subawards  
If the Federal agency applies a previous version, subaward must follow even if issued after 10/1/24



# Challenges with Equipment Thresholds



Difficult to simultaneously track these items for existing awards at the \$5,000 threshold.



Exemption granted in applying the 2024 Provisions for equipment and unused supplies



Recipients may instead use the revised equipment thresholds of \$10,000 provided in the 2024 Revisions **if permitted by the Federal agency that made the award.**



# 2024 Revisions and Single Audits

Single audit  
threshold increase  
from \$750,000 to  
\$1 million

Type A threshold  
to \$1 million

Modified  
definition of  
questioned costs

- Effective for non-Federal entities' fiscal year beginning on or after 10/1/24 (i.e. audits of fiscal year ending on or after September 30, 2025)



Do you think the exception allowed related to equipment thresholds is helpful for your institution?

- a) *Yes, this will ease our challenges with compliance*
- b) *No, there will still be challenges*
- c) *Unsure, we are still evaluating the impact on operations*





## Related Party Disclosures



# Related Party Disclosures

Financial Responsibility,  
Administrative Capability,  
Certification Procedures,  
Ability to Benefit; a Rule by  
the Education Department  
on 10/31/23

Federal Register :: Financial  
Responsibility,  
Administrative Capability,  
Certification Procedures,  
Ability To Benefit (ATB)



# Related Party Disclosures

Section 668.23(d)(1) –  
require the reporting of **all**  
related-party transactions  
in the notes to the financial  
statements

Requirement to disclose in  
the notes to the financial  
statements if there are **no**  
related-party transactions





Existing regulations require a broader set of disclosures than US GAAP



Level of detail that would allow the Secretary to readily identify the related party such as;

- Name
- Location and description of entity
- Nature and number of transactions (financial or otherwise)
- Routine de minimis transaction such as meals for board members do not need to be reported

# Related Parties Include:

**A.** **Affiliates** of the entity

**B.** **Entities for which investments in their equity securities would be required,** absent the election of the fair value option under the Fair Value Option Subsection of Section 825-10-15, to be accounted for by the equity method by the investing entity

**C.** **Trusts for the benefit of employees,** such as pension and profit-sharing trusts that are managed by or under the trusteeship of management



# Related Parties Include:

D.

**Principal owners** of the entity and members of their **immediate families**

E.

**Management** of the entity and members of their **immediate families**





# Related Parties Include:

F.

**Other parties with which the entity may deal** if one party controls or can significantly influence the management or operating policies of the other to an extent that one of the transacting parties might be prevented from fully pursuing its own separate interests

G.

**Other parties that can significantly influence** the management or operating policies of the transacting parties or that have an ownership interest in one of the transacting parties and can significantly influence the other to an extent that one or more of the transacting parties might be prevented from fully pursuing its own separate interests.





# Related Party Disclosures

## Affiliate

A party that, directly or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with an entity.

## Control

The possession, direct or indirect, of the power to direct or cause the direction of the management and policies of an entity through ownership, by contract, or otherwise.

## Management

Persons who are responsible for achieving the objectives of the entity and who have the authority to establish policies and make decisions by which those objectives are to be pursued.

# Common Examples

- 1 Donations from governance members
- 2 Donations from upper management
- 3 Investments accounted for under the equity method of accounting
- 4 Employee benefit trusts managed or trusteeship of management
- 5 Affiliates (for example, childcare center)
- 6 Expenditures to vendors meet the definition of related party



# Related Party Disclosures



## Transactions to be disclosed

- Activities (revenues and expenses)
- Assets
- Liabilities
- Off “balance sheet”



# Related Party Disclosures

## Name

- Trustee A?

## Location

- College location?

## Description

- Why are they a related party?

## Nature

- What type of transaction is it?



# Related Party Disclosures

Related Party	Location	Nature	Revenue (Expense)	Asset (Liability)	Other
Party A	Albany, NY	Contribution	750,000		
		Promise to Give		120,000	
Party B	Albany, NY				1,000,000
					22,000,000
Party C	Albany, NY	XY Defined Contribution Plan			See Note 7
Etc.					



# Related Party Disclosures

3

3 sets of financial statements?



No related party transactions?

# Related Party Disclosures



## Public institutions

- Announcement uses FASB definition of related party
- eZ audit edit check
- Other



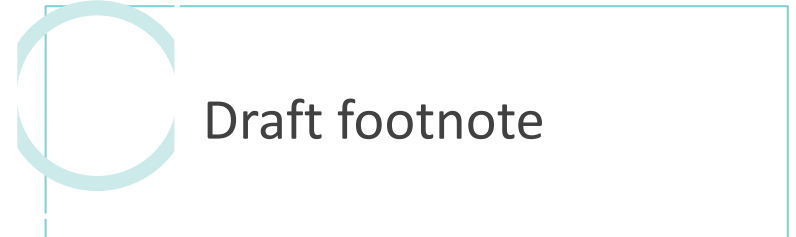
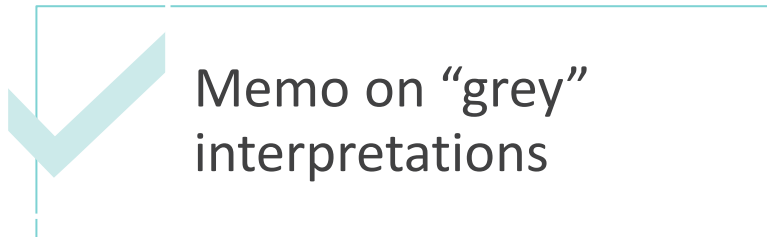
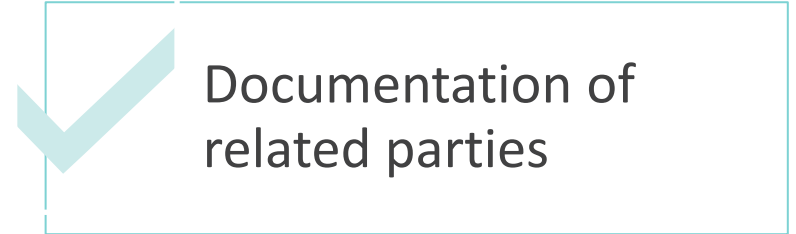
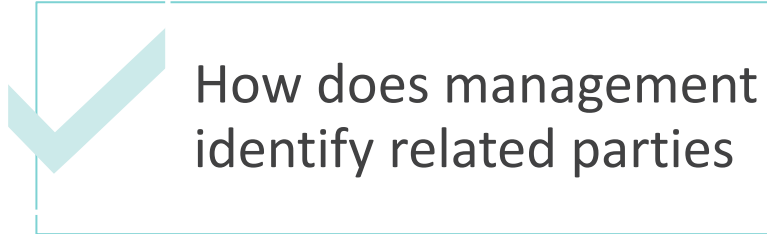
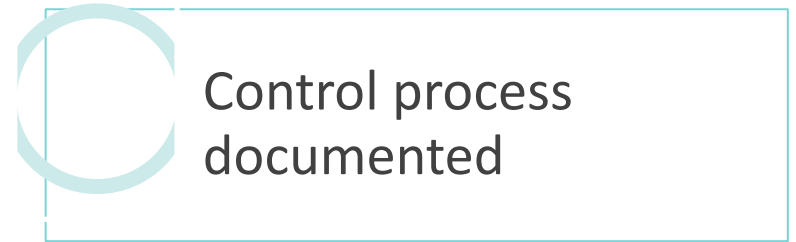
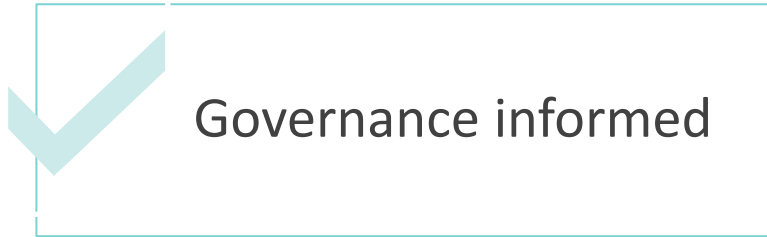
Letter from an official stating that the institution is backed by the full faith and credit of that government entity

- Title IV first time
- Recognition as public institution
- Upon request from ED



# Related Party Disclosures

## CHECK LIST



Which of the following is a related party that would need to be disclosed if my institution had transactions with it:

- a) *College mascot*
- b) *Trustee B has a board position at a company that does business with the College*
- c) *Head football coach*
- d) *Company that pays for the right to use College logos on apparel*





# Dear Colleague Letter



*Dear Colleague* – February 14, 2025

# Legal Requirements under the Civil Rights Act

*Discrimination on the basis of  
race, color, or national origin*

- ✓ Admissions
- ✓ Financial aid
- ✓ Hiring
- ✓ Training
- ✓ Institutional programming



# Dear Colleague – February 14, 2025

---

ED intends to take appropriate measures to assess compliance beginning not later than 14 days from 2/14/25

---

Ensure policies and actions comply with civil rights law

---

All  
institutions  
advised to;

Cease all efforts to circumvent prohibitions on the use of race to accomplish such ends

---

Cease reliance on third-party contactors, clearinghouses, or aggregators that are being used to circumvent prohibited uses of race

---

Failure to comply with civil rights law may face loss of federal funding



# Composite Score Calculations: Pre- and Post- Implementation Debt

(Nonprofit and Proprietary institutions only)



# Dear Colleague Letter: GEN-24-11

Issued December 20, 2024

Provides several scenarios to clarify how property, plant, and equipment (PP&E) and non-bond long-term debt are treated for the composite score calculation. It also provides alternative options for the treatment of bond long-term debt. In addition, it provides information about pre- and post-implementation leases.



*To address confusion regarding the correct manner in which to calculate the impact of long-term debt as it relates to PP&E for determining an institution's composite score.*



# Background

ED issued a Dear Colleague Letter allowing all long-term debt in the Primary Reserve Ratio, limited to the institution's PP&E.

**15 July 2003**

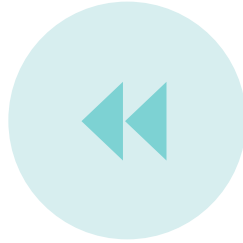
**23 Sep. 2019**

ED issued final regulations, superseding 2003 guidance and updating the composite score calculation, effective July 1, 2020.





# Debt Classification



## **PRE-IMPLEMENTATION DEBT:**

REPORTED IN FINANCIALS BEFORE  
7/1/20; CANNOT EXCEED PP&E  
RECORDED BEFORE 7/1/20.



## **POST-IMPLEMENTATION DEBT:**

REPORTED IN FINANCIALS AFTER 7/1/20.



# Refinanced Debt

## **Pre- Implementation Long-Term Debt:**

- Cannot exceed the book value of pre-implementation debt at the time of refinance.
- If proceeds are over this amount, classify the debt as post-implementation debt.

## **Post- Implementation Long-Term Debt:**

- Proceeds used for acquiring post-implementation PP&E qualify as post-implementation debt up to the book value of the new PP&E



# Additional Considerations



Does not need to be refinanced with the same lender/creditor.



Must reflect an arms-length transaction.



Cannot be a credit facility or related party debt.



Repayment terms can differ from the original debt (e.g., extended period, future balloon payment).



Costs of refinancing are not considered proceeds because the financial institution will pay any costs before proceeds are distributed.

How confident are you in applying the rules for refinancing debt as pre-implementation or post-implementation debt?

- a) *Very confident*
- b) *Somewhat confident*
- c) *Not confident*
- d) *Doesn't apply to me*



# Example 1

- Outstanding debt of \$85k refinanced for \$85k
- No new debt
- \$85,000 of the refinanced debt qualifies as *pre-implementation* long-term debt
  - No proceeds were received, and it does not exceed the book value of the PP&E

	<u>PPE</u>	<u>DEBT</u>
Pre-Implementation Balance	\$ 100,000	\$ 200,000
Depreciation	(10,000)	-
Payments on Debt	-	<u>(115,000)</u>
Post-Implementation Balance	\$ 90,000	\$ 85,000



# Example 1 (Subsequent Year- *original debt*)

- \$70,000 remaining balance of the refinanced debt qualifies as *pre-implementation* long-term debt
  - It does not exceed the current book value of the *pre-implementation* PP&E (\$80,000)

Subsequent Year	PPE	Debt
Pre-Implementation Balance	\$ 90,000	\$ 85,000
Depreciation	(10,000)	-
Payments on Debt	-	(15,000)
Post-Implementation Balance	\$ 80,000	\$ 70,000



# Example 1 (Subsequent Year- *new debt*)

- The \$40,000 of new long-term debt qualifies as *post-implementation* long-term debt because it does not exceed the current book value of the *post-implementation* PP&E (\$48,000).

New Layers	PPE	Debt
PPE purchases	\$ 50,000	\$ -
New debt	-	40,000
Depreciation	(2,000)	-
Payments on Debt	-	-
	\$ 48,000	\$ 40,000



# Example 1 (Subsequent Year- *new debt*)

- Only \$18,000 of the new long-term debt qualifies as *post-implementation* long-term debt
  - *Post-implementation* long-term debt cannot exceed the ending book value of the *post-implementation* PP&E (\$18,000)

New lease	PPE	Debt
PPE purchases	\$ 20,000	\$ -
New debt	-	20,000
Depreciation	(2,000)	-
Payments on Debt	-	-
	<u>\$ 18,000</u>	<u>\$ 20,000</u>





# Example 1 - Primary Reserve Ratio

## *Inputs*

- Pre-Implementation PPE  
\$80,000
- Post-Implementation PPE  
\$66,000
- Pre-Implementation Debt  
\$70,000
- Post-Implementation Debt  
\$58,000

## PRIMARY RESERVE RATIO

\$ 30,380	Net assets without donor restrictions
23,600	Net assets with donor restrictions
(17,600)	Net assets restricted in perpetuity
(1,000)	Donor restricted annuities, term endowments, life income funds
(146,000)	Property, plant, and equipment/Right-of-use of asset (pre- and post-implementation)
128,000	Debt for long-term purposes and lease obligations (pre- and post-implementation)
<b>\$ 17,380</b>	<b>Expendable Net Assets</b>
\$102,160	Total operating expenses
-	Sale of fixed assets (if loss)
<b>\$102,160</b>	<b>Total Expenses/Losses</b>

**0.1701 Primary Reserve Ratio**



## Example 2

- Outstanding debt of \$85k refinanced for \$90k
- No new PPE, no other new debt
- Even though BV of PPE is \$90k and debt is \$90k, none of the refinanced debt qualifies as pre-implementation since proceeds were received.

	<u>PPE</u>	<u>Debt</u>
Pre-Implementation Balance	\$ 100,000	\$ 200,000
Depreciation	(10,000)	-
Payments on Debt	-	(115,000)
Proceeds from refinancing	-	<u>5,000</u>
Post-Implementation Balance	\$ 90,000	\$ 90,000



# Example 2 - Primary Reserve Ratio

## *Inputs*

- Pre-Implementation PPE  
\$90,000
- Pre-Implementation Debt \$0

## PRIMARY RESERVE RATIO

\$ 30,380	Net assets without donor restrictions
23,600	Net assets with donor restrictions
(17,600)	Net assets restricted in perpetuity
(1,000)	Donor restricted annuities, term endowments, life income funds
(90,000)	Property, plant, and equipment/Right-of-use of asset (pre- and post-implementation)
-	Debt for long-term purposes and lease obligations (pre- and post-implementation)
<b>\$ (54,620)</b>	<b>Expendable Net Assets</b>
\$102,160	Total operating expenses
-	Sale of fixed assets (if loss)
<b>\$102,160</b>	<b>Total Expenses/Losses</b>
	<b>-0.5347 Primary Reserve Ratio</b>



# Example 2 - Primary Reserve Ratio

## *Inputs*

- Pre-Implementation PPE  
\$90,000
- Let's assume we re-financed and received no proceeds and pre-Implementation Debt  
\$85,000
- Primary reserve ratio from  
-.5347 to .2974

## PRIMARY RESERVE RATIO

\$ 30,380	Net assets without donor restrictions
23,600	Net assets with donor restrictions
(17,600)	Net assets restricted in perpetuity
(1,000)	Donor restricted annuities, term endowments, life income funds
(90,000)	Property, plant, and equipment/Right-of-use of asset (pre- and post-implementation)
85,000	Debt for long-term purposes and lease obligations (pre- and post-implementation)
<b>\$ 30,380</b>	<b>Expendable Net Assets</b>
\$102,160	Total operating expenses
-	Sale of fixed assets (if loss)
<b>\$102,160</b>	<b>Total Expenses/Losses</b>
	<b>0.2974 Primary Reserve Ratio</b>



# Example 3

- Outstanding debt of \$85k refinanced for \$90k
- No other new debt
- None of the refinanced debt qualifies as pre-implementation since proceeds were received. However, if \$5,000 proceeds used to purchase PPE of \$4,500, then \$4,500 is post-implementation debt

	PPE	Debt
Pre-Implementation Balance	\$ 100,000	\$ 200,000
Depreciation	(10,000)	-
Payments on Debt	-	(115,000)
Proceeds from refinancing	-	5,000
Post-Implementation Balance	\$ 90,000	\$ 90,000



# Bond Refinancing (Restricted for PPE)

- **Qualification:** If bond refinancing results in proceeds restricted for PPE, the bond may qualify as post-implementation debt under certain conditions.
- **Disclosures:** Requires additional note disclosures and specific presentation in financial statements.
- **Documentation:** Supporting documentation must be submitted with eZ-Audit.
- **Guidance:** The Department expects to issue an Electronic Announcement for additional guidance.



# Leases



December 15, 2018, is the date to distinguish between pre- and post-implementation leases.



May opt out of differentiating between pre- and post- but cannot change distinction once made.

If this distinction was not made in first year of 2016-02 adoption, Department will assume it has opted out.



# Triggering Events





# Triggering Events

Intended to inform the Department of Education when precarious situations are likely, imminent or ongoing.

Part of Financial Responsibility rules



# Triggering Events

## Mandatory (14)

- Clearly defined and can lead to automatic intervention

## Discretionary

- More loosely defined and allow ED to assess responsibility for each occurrence



# Triggering Events

Event	Result
Institution with composite score less than 1.5 is required to pay a debt or incurs a liability from settlement that results in recalculated score of less than 1.0	Failure of financial responsibility
Lawsuit after 7/1/24 by Federal or State authorities in which the Federal Government has intervened	Automatic failure
Process of change in ownership must pay a debt or settlement at any point through second full year	Failure if recalculated composite score less than 1.0



# Triggering Events

Event	Result
Condition in agreements with creditor that could result in a default or adverse condition due to an action by ED or a creditor terminates	Automatic failure
Formal declaration of financial exigency	Automatic failure
Enter into receivership	Automatic failure
ED initiates a proceeding to recoup the cost of approved borrower defense claims	Failure if recalculated composite score less than 1.0



# Triggering Events

Event	Result
50% of title IV, HEA aid received for programs that fail GE thresholds	Automatic failure
Two most recent official CDRs are 30 percent or greater	Automatic failure
Required to submit teach-out plan by State, ED or another agency or oversight body for reasons related to financial concerns	Automatic failure



# Triggering Events

Event	Result
Proprietary institution did not meet 10% of revenue from sources other than federal educational assistance	Automatic failure
Proprietary institution with score less than 1.5 has a withdrawal of owners equity that results in a score less than 1.0	Failure if recalculated score less than 1.0
Institutions with 50% ownership listed on a public exchange not in compliance with listing requirements	Automatic failure
Institution receives a contribution in last quarter, then makes a distribution in first quarter resulting in score less than 1.0	Automatic failure



# Discretionary

- Accreditor actions
- Other creditor events
- Fluctuations in title IV volume
- High dropout rate
- Interim reporting
- Pending borrower defense claims
- Program discontinuation
- Location closures
- State actions
- Loss of institutional or program eligibility
- Exchange disclosures
- Actions by another Federal agency
- Other teach-out plans
- Other events or conditions



# Triggering Events

Reporting

- Generally, 21 days from a point defined in section 668.171(f)

Trigger happens

- Irrevocable letter of credit
- Cash escrow
- Not less than 10% of total Title IV; can stack protection up to 50% for each failed trigger
- May not be required if institution can demonstrate event has been resolved or insurance covers loss





# Triggering Events



## Public institutions

- **Section 668.171(g)(C)(iv)**
  - Public schools violate financial responsibility requirements if they meet the criteria of automatic or discretionary triggering events
  - Financial protection not required
  - Additional reporting requirements such as heightened cash monitoring



# GASB Standards



# GASB 100 Accounting for Changes and Error Corrections



Effective date

**June 30, 2024**



## **New requirements:**

Updated disclosure guidance for:

- Accounting principles
- Accounting estimates
- Correction of errors

Required to disclose line items impacted by the change even if beginning balances remain the same



## **CLA can help**

By assisting with or evaluating financial statement disclosure updates



# GASB 101 Compensated Absences



Effective date

**December 31, 2024**



## Updated framework

- Reevaluate leave policies
- Liability must include any accumulated leave that is unused or used but unpaid
- Footnote disclosures will be enhanced



## Examples include

- Sick leave not paid at termination
- Parental leave
- Military leave and jury duty that has commenced



## CLA can help

By evaluating the standard related to compensated absences and assisting with or evaluating in financial statement disclosures



# GASB 102 Certain Risk Disclosures

**CLA can help**  
By assisting with or  
evaluating financial  
statement disclosure  
updates



Effective date

**June 30, 2025**



## **Increased footnote disclosures surrounding risk:**

- Limitations on raising revenues
- Concentrations related to tax revenue or vendors
- Debt or mandated spending — especially unfunded mandates
- Impact of major employer leaving the community
- Collective bargaining agreements



# GASB 103 Financial Reporting Module

**CLA can help**  
By assisting with or  
evaluating financial  
statement disclosure  
updates



Effective date

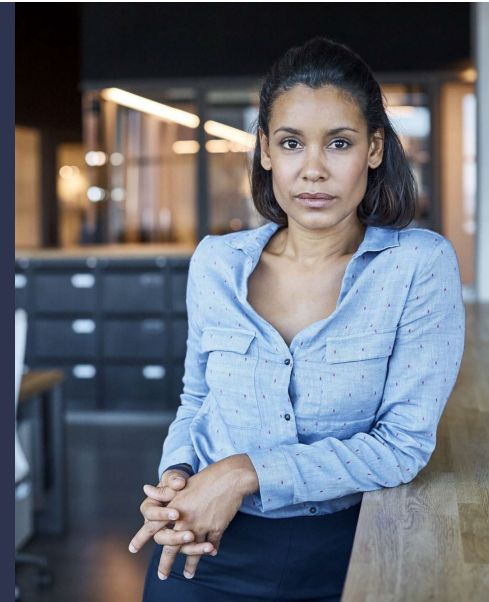
**June 30, 2026**



## **Impacts financial statement presentation**

Updated disclosure guidance for:

- MD&A consistency
- Clearer definition of unusual or infrequent items
- Presentation of proprietary fund statements
- Major component unit information
- Budgetary comparison information



# GASB 104 – Disclosure of Certain Capital Assets



Effective date

**June 30, 2026**



**Will clarify how capital assets are disclosed in financials:**

- Capital assets held for sale and related pledged debt
- Leased assets
- Subscription assets
- Right to Use PPP assets
- Other intangible assets



**CLA can help**

By assisting with or evaluating financial statement disclosure updates





# FASB Standards

Standards Effective for 2024 Year Ends or  
Able to be Early Adopted





# ASU 2020-06 Debt



Effective date

**December 31, 2024**



## **Debt with conversion and other options**

- For convertible debt, there may be a positive income boost
- Interest expense will be more reflective of the contractual interest rate
- Enhanced disclosures



**Consult as needed**



# ASU 2021-08 Business Combinations



Effective date

**December 31, 2024**



## **Accounting for contract assets and liabilities**

- An acquirer needs to account for acquired revenue contracts under ASC 606 as if it had originated the contracts versus fair valuing the related contract assets and liabilities
- Requires reviewing the correct application of ASC 606 to the acquired revenue contacts



# ASU 2022-01 Derivatives and Hedging

Consult as needed



Effective date

**December 31, 2024**



## Fair Value Hedging – Portfolio Layer Method

- **Before ASU 2022-01:** Only prepayable financial assets could be included in a closed portfolio hedged using the last-of-layer method.
- **After ASU 2022-01:** Both prepayable and non-prepayable financial assets can be included in a closed portfolio hedged using the portfolio layer method.



# ASU 2023-01 Leases

Likely already adopted,  
otherwise CLA can  
help!



Effective date

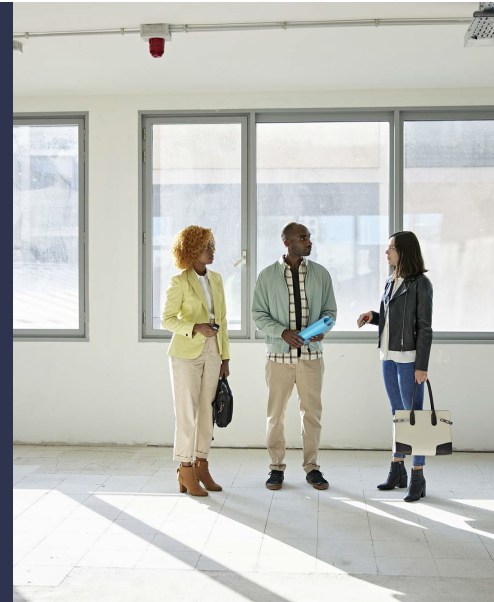
**December 31, 2024**

Early Adoption is Permitted



## Common control arrangements:

- Practical expedient to use written terms (if they exist) to determine existence, accounting, and classification of a lease
- Provides for amortizing leasehold improvements over the useful life of the improvements to the common control group (regardless of the lease term)



# 2023-02 Investments — Equity Method

Consult as needed



Effective date

**December 31, 2025**

Early Adoption is Permitted



## **Accounting for investments in tax credit structures using the proportional amortization method**

- Permits reporting entities to elect to account for their tax equity investments, regardless of the tax credit program
- Allowed to use the proportional amortization method if certain conditions are met



# 2023-05 Business Combinations

**CLA can help**  
By evaluating the  
standard on  
joint ventures



Effective date

**December 31, 2025**

Early Adoption is permitted



## **Joint venture formations — combinations beginning January 1, 2025**

- Requires new basis of accounting upon formation
- Recognize and initially measure its assets and liabilities at fair value
- Minor exceptions consistent with the business combinations guidance



# 2023-08 Intangibles

Consult if Applicable



Effective date

**December 31, 2025**

Early Adoption is Permitted



## Goodwill and other — crypto assets

- Application mainly in client accounting and advisory services nonattest environments
- Require an entity measure crypt assets at fair value in the statement of financial position
- Recognize changes from remeasurement in net income
- Enhanced disclosures



# ASU 2023-09 Income Taxes

Early adoption is not expected



Nonpublic Entities  
Effective date

**December 31, 2026**

Early Adoption is Permitted



**Requires ALL entities to qualitatively disclose information of reconciling items between the statutory tax rate and effective tax rate**



**Most of the standard is for public companies**



**All entities must disclose additional information about income tax expense, income taxes paid, and segregation of taxes paid to individual jurisdictions**





# 2024-01 Compensation



Effective date

**December 31, 2026**

Early Adoption is Permitted

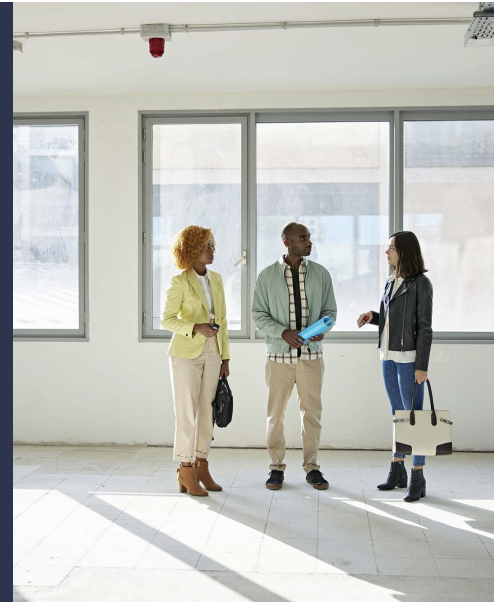


## Stock Compensation - Determining the Current Price of an Underlying Share for Equity-Classified Share-Based Awards

- Simplifies the process for determining the fair value of share-based awards.
- Provides a practical expedient for nonpublic companies to determine the “current price input” of equity-classified share-based payment awards

## CLA can help

By evaluating management’s policy and controls over valuing the current price input.



# 2024-04 Debt with Conversion and Other Options

Consult as needed



Effective date

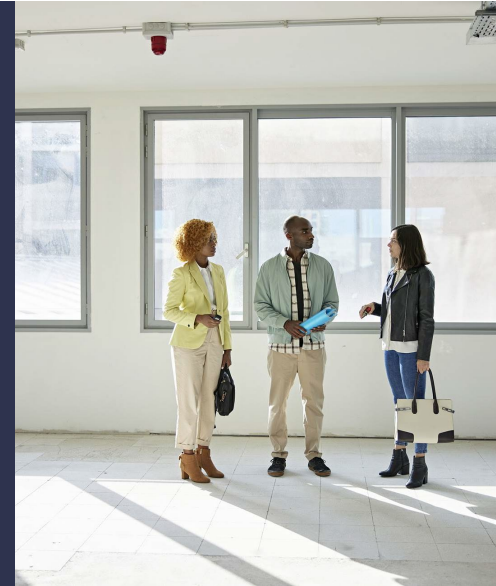
Annual reporting periods after  
**December 15, 2025**

Early Adoption is Permitted for  
those that adopted ASU 2020-06



## Induced Conversions of Convertible Debt Instruments

- Affects entities that settle convertible debt instruments for which the conversion privileges were changed to induce conversion.
- Clarifies the requirements for determining whether certain settlements of convertible debt instruments should be accounted for as an induced conversion versus a debt extinguishment





# Break

12:00 – 12:10 p.m. CT

*\*please note, we will be doing a sound check with our speakers during this time.  
The next session will start at 12:10 p.m.*





# Future-Ready

Generational Diversity and Hybrid Work



# Learning Objectives

---

Recognize the dynamics of generational diversity in the workforce

---

Discuss strategies for adapting to hybrid work environments in higher education

---

Identify how college leaders are navigating rapid workplace transformations with innovation and resilience



How much of your  
workforce is  
remote/hybrid?

- a) *Very little*
- b) *Moderate*
- c) *Head football coach*
- d) *Significant, and I'd like CLA to contact me to discuss how they can help*





# Break

12:40 – 12:50 p.m. CT

*\*please note, we will be doing a sound check with our speakers during this time.  
The next session will start at 12:50 p.m.*





# Game On

Understanding the NIL and NCAA Reforms





# Learning Objectives

---

Describe the recent changes in NIL (Name, Image, Likeness) policies and NCAA regulations

---

Discuss the impact of these changes on college sports and athlete recruitment



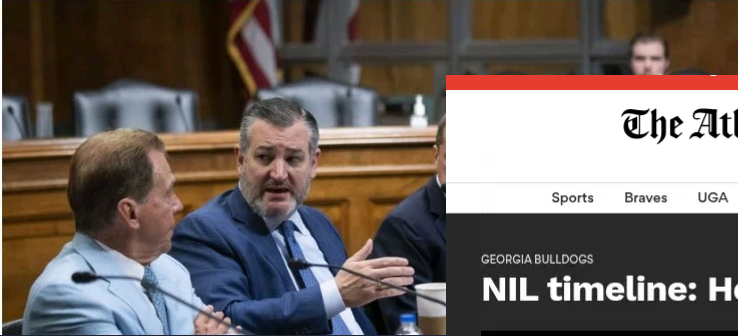
How effective has your institution been at addressing NIL and changes in athletics?

- a) *Very effective*
- b) *Somewhat effective*
- c) *We are not making progress, and I would like CLA to contact me to discuss how they can help.*



# Saban shares views on NIL, transfer rule on Capitol Hill

MARCH 13, 2024 • NEWS



## NCAA board votes to accept antitrust settlement, sources say

Pete Thamel and Dan Murphy  
May 22, 2024, 09:36 PM ET

Share Like

395

The NCAA's Board of Governors voted Wednesday evening to agree to settlement terms in... sources, sources told ESPN, joining three power... with a historic change for the way college sports

## The Atlanta Journal-Constitution

Sports

Sports Braves UGA Hawks Georgia Tech Falcons United High School Sports

GEORGIA BULLDOGS

## NIL timeline: How we got here and what's next

COLLEGE FOOTBALL

NCAA Pac-12 Conference

Add Topic +

## What happened to the Pac-12? Explaining the fall and rebuild for former Power Five league



Austin Curtright

USA TODAY NETWORK

Published 6:05 a.m. ET Jan. 1, 2025 | Updated 11:28 a.m. ET Jan. 21, 2025



POLICY

## The NCAA's proposal to pay college athletes is fair. That's the problem.

The end of amateurism finally comes for college sports. Will we miss it?

by Bryan Walsh

May 29, 2024, 5:15 AM MDT



# Agenda

## Timeline of Changes in NCAA Athletics

- NIL
- Transfer Portal
- Conference Realignment

## Panel Discussion

- Challenges
- How schools are pivoting

## Conclusion

- Best practices
- How CLA can help



# *Disclaimer*

This topic is rapidly developing, and new information is released frequently. Recent legal rulings and other ongoing litigation can impact how schools are currently operating. This presentation was given with our knowledge of the current state of NIL and NCAA bylaws.



# Introductions



*Ben Cahill, CPA, Principal*

13 years of public accounting experience (10 years with CLA).

Focused on professional and collegiate athletes since 2016. (CLA collaborates with over 200 current and retired professionals).

Played college golf (NCAA) at St. John's University (MN).



*Jean Bushong, CPA, Principal*

Has worked with higher education institutions for almost 30 years.

Performs agreed-upon-procedures for NCAA .

College sports fan!



# Our Panel



**Jacquie Bruns**  
Deputy Athletic  
Director, CFO, Senior  
Woman Administrator



**Cory Hilliard**  
Sr Associate Athletic  
Director, Business Ops,  
Chief Athletic Financial  
Officer



**Tim McCleary**  
Sr Associate Athletic  
Director, Business  
Ops and Planning,  
CFO



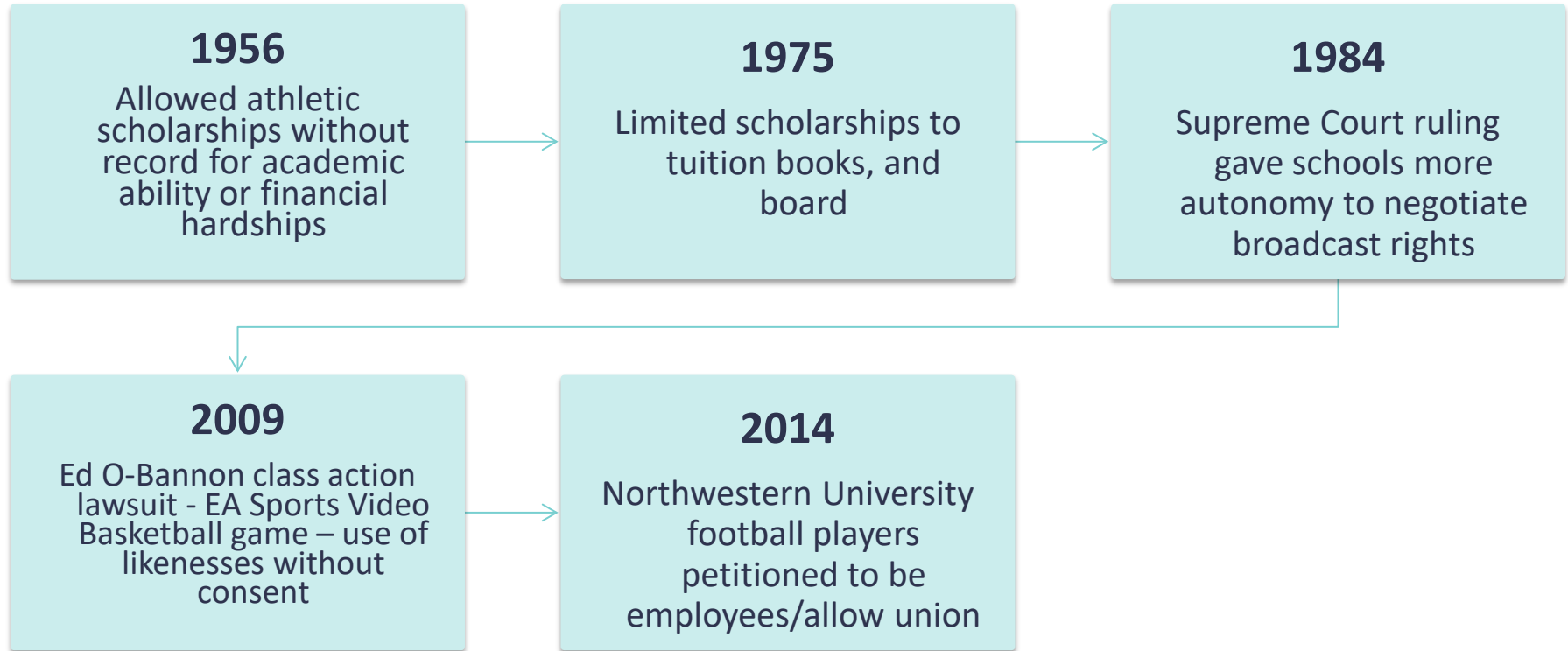


# Background and Timeline





# Timeline of NCAA Athletics Changes – *the beginning*



# Timeline of NCAA Athletics Changes – *Now*



# What Is NIL?

## NIL = Name, Image, and Likeness

Prior to 2021, NCAA rules **prohibited** student-athletes from profiting on their name, image and likeness

Generally, includes things like **endorsements, commercials, appearances, autograph signings, social media posts and advertisements**, and other **business activities - youth camps**

NIL deals are not direct payments from universities (paying student-athletes) but **compensation by third parties**




# What are NIL Collectives?

Organizations established by boosters and fans of a university's athletic program to develop and fund or otherwise facilitate **NIL deals** for student-athletes



# NCAA v House Settlement

 Backpay of \$2.6 billion to be paid to students competing from 2016 – 2024.



Future athlete revenue sharing

*Permissive, not required*



Eliminates scholarship limits



Roster limits



NIL third-party deals must be approved through a clearinghouse



# Changes = *Challenges*

## **Name, Image, Likeness**

Students could now be paid, but many rules and tax implications.

## **Conference Realignment**

Future budgets significantly impacted. How to properly plan?

## **House Settlement**

Title IX implications?

## **House Settlement**

Athlete payment - employee?

## **House Settlement**

Roster limits could harm athletes who want to compete.

## **Recruiting**

While NIL is not to be used in recruiting; difficult to enforce.

## **Transfer Portal**

Athlete instability; players transferring for financial incentives.

## **Various Changes**

Updating systems and monitoring to keep up with changes.





# Panel Discussion



# Panel Discussion



**Jacque Bruns**

Deputy Athletic Director, CFO,  
Senior Woman Administrator



**Cory Hilliard**

Sr Associate Athletic Director,  
Business Ops,  
Chief Athletic Financial Officer



UNIVERSITY OF MINNESOTA



**Tim McCleary**

Sr Associate Athletic Director,  
Business Ops and Planning, CFO





# Closing Remarks



# How CLA can help

- Educational classes
- Tax assistance
- Revenue projections
- Employee vs contractor tax compliance
- Budgeting





# Questions?



*Thank you!*

Ben Cahill, Principal

[ben.cahill@CLAconnect.com](mailto:ben.cahill@CLAconnect.com)

(320) 203-5511

Jean Bushong

[jean.bushong@CLAconnect.com](mailto:jean.bushong@CLAconnect.com)

(303) 265-7884



CLAconnect.com



CPAs | CONSULTANTS | WEALTH ADVISORS

©2025 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAglobal.com/disclaimer](https://www.claglobal.com/disclaimer). Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



# Break

2:00 – 2:05 p.m. CT

*\*please note, we will be doing a sound check with our speakers during this time.  
The next session will start at 2:05 p.m.*





# Ethical Hacking

A Primer on Penetration Testing for Non-IT Professionals



# Learning Objectives

---

Recognize the fundamentals of penetration testing: Gain a foundational understanding of what penetration testing entails, its purpose, and its importance in the cybersecurity landscape

---

Discuss real-world case studies: Recall case studies that demonstrate the practical application of penetration testing in real-world scenarios, highlighting successes and lessons learned

---

Recognize compliance considerations: Discuss the compliance requirements associated with penetration testing and conducting activities ethically



How often is your institution performing a penetration test?

- a) *Annually*
- b) *Once in a while*
- c) *Not sure, but we have enough resources to handle it internally*
- d) *Not sure, and I would like CLA to contact me to discuss how they can help*





# Raise Your Hand if You Work for a Tech Company

Security Cameras

Motion Sensors

Automated Lighting

Print Vendors

Smart TV Displays

HVAC

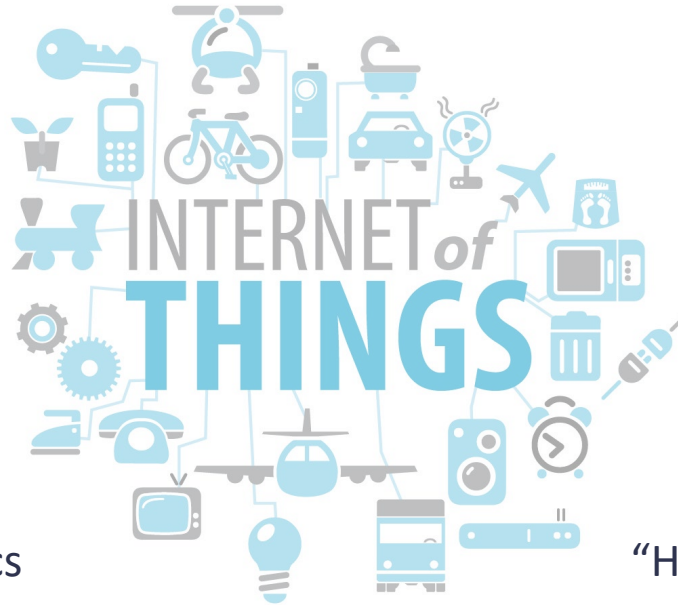
Controllers and PLCs

Digital Assistance

Cloud Applications & Analytics

Bio-Medical Care & Monitoring

**“Presence”**



Security cameras

Garage door

Home thermostat

Cable TV remote

Smart TV

Sleep number bed

Roomba

Apple Watch or FitBit

“Hey Siri, what’s my balance?”

**“Presence”**

Stand Up If...





# What is a Penetration Test?

- A process to evaluate the security of a system by simulating a cybersecurity attack.
- Key goals include:
  - **Validating expectations** related to security are aligned
  - Objective, independent, and expert **evaluation of the systems security** - sometimes done for quality control
  - **Identify and verify vulnerabilities** and their exploitability
  - Quantify and qualify the **risk** of individual / discreet vulnerabilities and the **impact** they may have to individual systems and the organization as a whole



# Governance, Compliance and Risk Management

A wide variety of regulatory compliance and governance frameworks require penetration testing. Examples include:

- GLBA, FTC, HIPAA, NERC/CIP – Regulatory requirements
- PCI-DSS, CMMC, SOC – Contractual obligations
- NIST, CIS, HITRUST, ISO – Governance frameworks

Testing can follow any or a combination of the following:

- Collaborative vs uniformed  
“White box” vs “Black box”
- Red Team, Blue Team, Purple Team  
“Capture the flag”

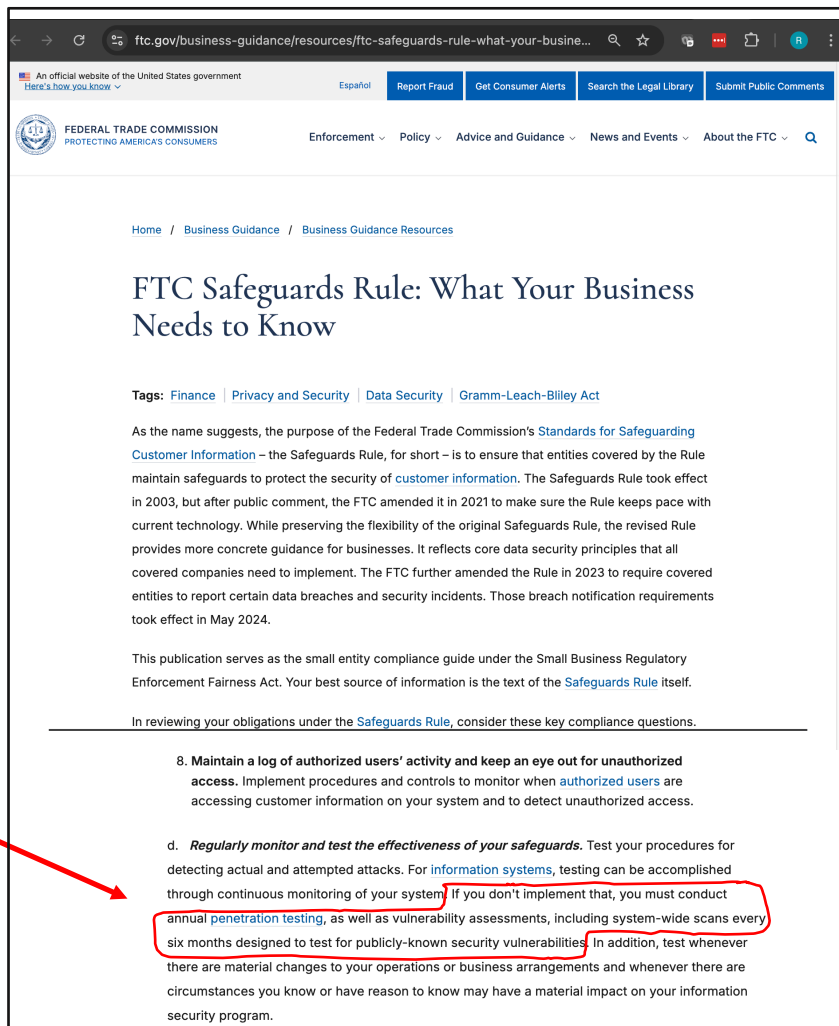


# Regulatory

## GLBA and the FTC Safeguards rule require penetration testing

- Penetration testing required once per year AND after significant changes.
- System wide vulnerability assessments every 6 months...

<https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know>

A screenshot of the Federal Trade Commission's website page titled "FTC Safeguards Rule: What Your Business Needs to Know". The page includes a navigation bar with links for "Report Fraud", "Get Consumer Alerts", "Search the Legal Library", and "Submit Public Comments". The main content area features the title "FTC Safeguards Rule: What Your Business Needs to Know" and a list of tags: "Finance", "Privacy and Security", "Data Security", and "Gramm-Leach-Bliley Act". The text explains the purpose of the rule and its history. A red arrow points from the text in the slide to a specific section of the webpage. In this section, the text states: "8. Maintain a log of authorized users' activity and keep an eye out for unauthorized access. Implement procedures and controls to monitor when authorized users are accessing customer information on your system and to detect unauthorized access." Underneath, item "d." reads: "Regularly monitor and test the effectiveness of your safeguards. Test your procedures for detecting actual and attempted attacks. For information systems, testing can be accomplished through continuous monitoring of your system. If you don't implement that, you must conduct annual penetration testing, as well as vulnerability assessments, including system-wide scans every six months designed to test for publicly-known security vulnerabilities. In addition, test whenever there are material changes to your operations or business arrangements and whenever there are circumstances you know or have reason to know may have a material impact on your information security program." The phrases "annual penetration testing" and "every six months" are circled in red in the screenshot, corresponding to the text in the slide.

ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-busine...  
An official website of the United States government  
Here's how you know  
Español Report Fraud Get Consumer Alerts Search the Legal Library Submit Public Comments  
FEDERAL TRADE COMMISSION  
PROTECTING AMERICA'S CONSUMERS  
Enforcement Policy Advice and Guidance News and Events About the FTC  
Home / Business Guidance / Business Guidance Resources  
FTC Safeguards Rule: What Your Business Needs to Know  
Tags: Finance | Privacy and Security | Data Security | Gramm-Leach-Bliley Act  
As the name suggests, the purpose of the Federal Trade Commission's [Standards for Safeguarding Customer Information](#) – the Safeguards Rule, for short – is to ensure that entities covered by the Rule maintain safeguards to protect the security of [customer information](#). The Safeguards Rule took effect in 2003, but after public comment, the FTC amended it in 2021 to make sure the Rule keeps pace with current technology. While preserving the flexibility of the original Safeguards Rule, the revised Rule provides more concrete guidance for businesses. It reflects core data security principles that all covered companies need to implement. The FTC further amended the Rule in 2023 to require covered entities to report certain data breaches and security incidents. Those breach notification requirements took effect in May 2024.  
This publication serves as the small entity compliance guide under the Small Business Regulatory Enforcement Fairness Act. Your best source of information is the text of the [Safeguards Rule](#) itself.  
In reviewing your obligations under the [Safeguards Rule](#), consider these key compliance questions.  
8. **Maintain a log of authorized users' activity and keep an eye out for unauthorized access.** Implement procedures and controls to monitor when [authorized users](#) are accessing customer information on your system and to detect unauthorized access.  
d. **Regularly monitor and test the effectiveness of your safeguards.** Test your procedures for detecting actual and attempted attacks. For [information systems](#), testing can be accomplished through continuous monitoring of your system. If you don't implement that, you must conduct [annual penetration testing](#), as well as vulnerability assessments, including system-wide scans every six months designed to test for publicly-known security vulnerabilities. In addition, test whenever there are material changes to your operations or business arrangements and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

# Contractual

## PCI Penetration Testing Guidance

- Penetration testing required once per year AND after significant changes
  - External and Internal
- Guidance on how to define scope, types of testing, and how to perform testing

Table of Contents	
<b>1 Introduction</b>	<b>4</b>
1.1 Objective	4
1.2 Intended Audience	4
1.3 Terminology	4
1.4 Navigating this Document	5
<b>2 Penetration Testing Components</b>	<b>6</b>
2.1 How does a penetration test differ from a vulnerability scan?	6
2.2 Scope	7
2.2.1 External Penetration Test	8
2.2.2 Internal Penetration Test	8
2.2.3 Testing Segmentation Controls	8
2.2.4 Critical Systems	9
2.3 Application-Layer and Network-Layer Testing	9
2.3.1 Authentication	9
2.3.2 PA-DSS Compliant Applications	9
2.3.3 Web Applications	10
2.3.4 Separate Testing Environment	10
2.4 Segmentation Checks	10
2.5 Social Engineering	11
2.6 What is considered a "significant change"?	11
<b>3 Qualifications of a Penetration Tester</b>	<b>12</b>
3.1 Certifications	12
3.2 Past Experience	12
<b>4 Methodology</b>	<b>14</b>
4.1 Pre-Engagement	14
4.1.1 Scoping	14
4.1.2 Documentation	14
4.1.3 Rules of Engagement	15
4.1.4 Third-Party-Hosted / Cloud Environments	16
4.1.5 Success Criteria	16
4.1.6 Review of Past Threats and Vulnerabilities	16
4.1.7 Avoid scan interference on security appliances	17
4.2 Engagement: Penetration Testing	17
4.2.1 Application Layer	18
4.2.2 Network Layer	18
4.2.3 Segmentation	19
4.2.4 What to do when cardholder data is encountered	19

[https://docs-prv.pcisecuritystandards.org/Guidance%20Document/Penetration%20Testing/Penetration-Testing-Guidance-v1\\_1.pdf](https://docs-prv.pcisecuritystandards.org/Guidance%20Document/Penetration%20Testing/Penetration-Testing-Guidance-v1_1.pdf)



# Standards Framework

## CIS Critical Controls Version 8

<b>CONTROL 01</b> Inventory and Control of Enterprise Assets 5 Safeguards   101 2/5   102 4/5   103 5/5	<b>CONTROL 02</b> Inventory and Control of Software Assets 7 Safeguards   101 3/7   102 6/7   103 7/7	<b>CONTROL 03</b> Data Protection 14 Safeguards   101 6/14   102 12/14   103 14/14
<b>CONTROL 04</b> Secure Configuration of Enterprise Assets and Software 12 Safeguards   101 7/12   102 11/12   103 12/12	<b>CONTROL 05</b> Account Management 6 Safeguards   101 4/6   102 6/6   103 6/6	<b>CONTROL 06</b> Access Control Management 8 Safeguards   101 5/8   102 7/8   103 8/8
<b>CONTROL 07</b> Continuous Vulnerability Management 7 Safeguards   101 4/7   102 7/7   103 7/7	<b>CONTROL 08</b> Audit Log Management 12 Safeguards   101 3/12   102 11/12   103 12/12	<b>CONTROL 09</b> Email and Web Browser Protections 7 Safeguards   101 2/7   102 6/7   103 7/7
<b>CONTROL 10</b> Malware Defenses 7 Safeguards   101 3/7   102 7/7   103 7/7	<b>CONTROL 11</b> Data Recovery 6 Safeguards   101 4/5   102 5/5   103 5/5	<b>CONTROL 12</b> Network Infrastructure Management 8 Safeguards   101 1/8   102 7/8   103 8/8
<b>CONTROL 13</b> Network Monitoring and Defense 11 Safeguards   101 0/11   102 6/11   103 11/11	<b>CONTROL 14</b> Security Awareness and Skills Training 9 Safeguards   101 8/9   102 9/9   103 9/9	<b>CONTROL 15</b> Service Provider Management 7 Safeguards   101 1/7   102 4/7   103 7/7
<b>CONTROL 16</b> Applications Software Security 14 Safeguards   101 0/14   102 11/14   103 14/14	<b>CONTROL 17</b> Incident Response Management 9 Safeguards   101 3/9   102 8/9   103 9/9	<b>CONTROL 18</b> Penetration Testing 5 Safeguards   101 0/5   102 3/5   103 5/5

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	101	102	103
18.1	<b>Establish and Maintain a Penetration Testing Program</b>  Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.	N/A	Identify	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18.2	<b>Perform Periodic External Penetration Tests</b>  Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.	Network	Identify	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18.3	<b>Remediate Penetration Test Findings</b>  Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	Network	Protect	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18.4	<b>Validate Security Measures</b>  Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	Network	Protect	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
18.5	<b>Perform Periodic Internal Penetration Tests</b>  Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.	N/A	Identify	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



# Standards and Defined Processes

There are a variety of standards for penetration testing

- NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)
- PCI-DSS (Payment Card Industry Data Security Standard)
- OWASP (Open Worldwide Application Security Project)
- OSSTMM (Open Source Security Testing Methodology Manual)
- PTES (Penetration Testing Execution Standard)

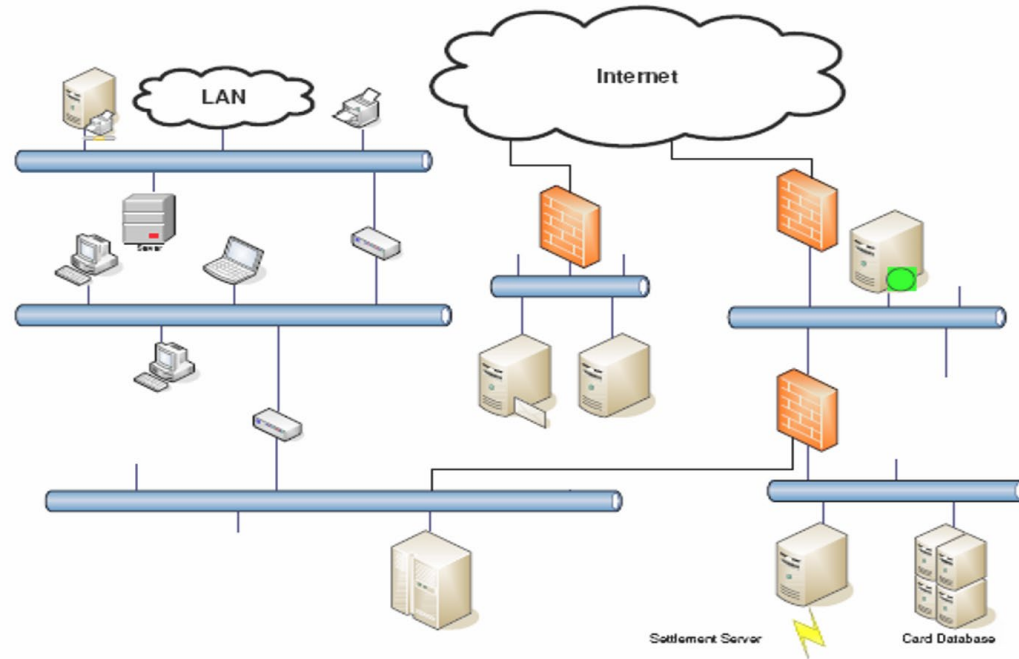
These define how to do the testing (hint: they all say largely the same thing...)





# How Do We Define the Scope?

- Defining the scope and process depends on a number of factors:
  - ✓ Goals and objectives
  - ✓ Size and complexity
  - ✓ What are the assets that need to be protected



# Stages of a Penetration Testing

- Planning
- Information Gathering
- Vulnerability assessment and scanning
- Manual testing, exploitation, privilege escalation, lateral movement, and persistence
- Reporting
- Retesting



# Execution of a Penetration Test

- The preceding slides culminate in one or more the of the following assessment "types"

## External Penetration Testing

- In-house Infrastructure, websites and applications, email and remote desktop
- Cloud hosted infrastructure and applications

## Social Engineering Testing

- Spear Phishing
- Pre-text calls (Vishing)
- On-site/in-person social engineering

## Internal Network Penetration

- Firewalls, routers, wireless, infrastructure
- Servers, applications, automated systems
- Workstations and peripherals

## Custom Penetration Testing

- Hardware and device penetration testing
- Application penetration testing



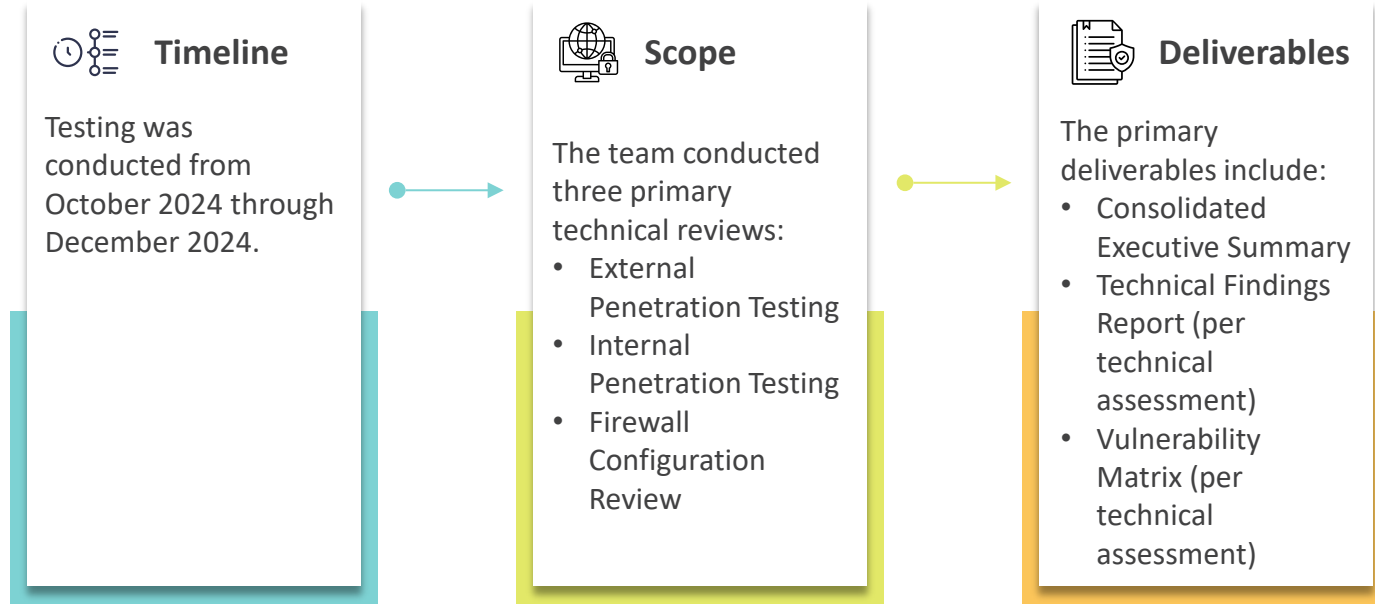


# Case Study



# Engagement Overview

In Q4 of 2024 multiple technical assessments to assess the organization's current security posture and develop a strategic roadmap for future state enhancements.



# Key Themes and Potential Risks

During the engagement, the team identified key themes and examples of areas of improvement to consider as you enhance your overall security posture.

## Configuration Management

- Multiple instances of weak and/or outdated services
- Configuration file with clear text passwords on the internal network

## Patch Management

- Outdated systems and software present in the environment
- Unsupported operating systems were present in the environment

## Network Configuration

- Demilitarized Zone (DMZ) not being utilized
- Legacy protocols are vulnerable to attack
- Internal network is not segmented to restrict traffic flow

## Password Management

- 65% of passwords in use were cracked, including 10 privileged users
- Default credentials were found on systems



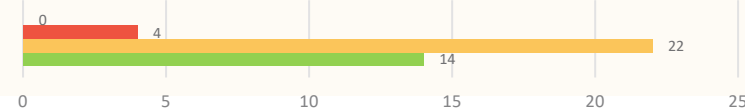
# Assessment Results - Ext. Penetration Test

Based on the assessment of the external attack surface, the team identified the following vulnerabilities.

## Scope

- Public IP Addresses (11.222.333.44/27)
- Employees via Spear Phishing Exercise

## Findings Summary



## Summary of Findings

### Findings:

Default / weak configuration settings on externally exposed systems  
Phishing simulation resulted in unauthorized access

**Details:** Several internet-exposed systems had misconfigurations:

- Weak encryption protocols/ciphers/certificates
- Insecure configuration settings and file transfer services on web services
- Staff provided credentials and ran executable code from phishing link(s)

**Recommended Remediation:** Improve processes to harden configuration standards to any system that is exposed to the internet.

- Harden web applications and enable strong encryption
- Use secure file transfer services
- Train and test users through automated services and penetration testing

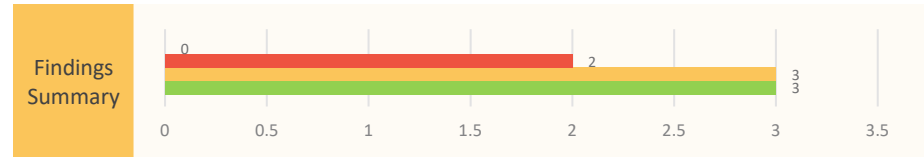
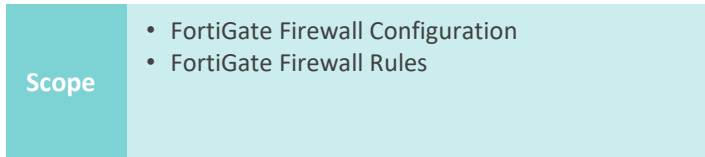
## Key Focus Area



45% of the external vulnerability findings were sourced from 11.222.333.xx (<https://portal.sample.com/Default.aspx>)

# Assessment Results - Firewall Penetration Test

Based on the assessment of the in-scope firewalls, the team identified the following vulnerabilities.



## Summary of High-Risk Findings

### Finding: Lack of Internal Network Segmentation

**Details:** The firewall policy is currently configured to allow unrestricted access to all zones within the network (including more than one previously unknown “any-any” rule).

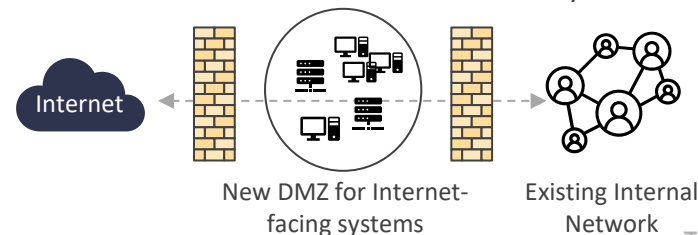
**Recommended Remediation:** Develop network segments based on function and risk and then restrict access to these segments based on business need.



### Finding: Lack of Demilitarized Zone (DMZ)

**Details:** The firewall policy supports a DMZ, however none of the public facing services currently utilize it, placing internet-facing systems on the same network as internal assets.

**Recommended Remediation:** Place internet-facing systems within the DMZ to isolate them from internal systems.





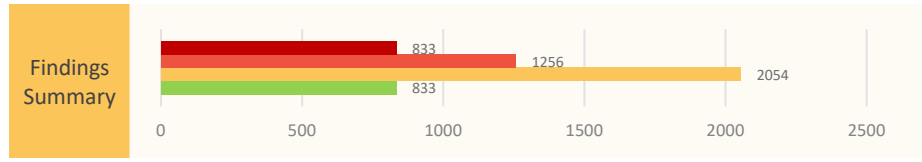
- Critical
- High
- Medium
- Low

# Assessment Results - Internal Penetration Test

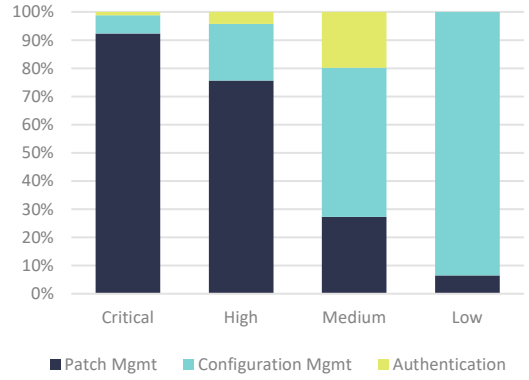
Based on the assessment of the internal environment, the team identified the following vulnerabilities.

**Scope**

- SAMPLE.local
- 172.30.0.0/21
- 192.168.0.0/21



## Finding Categories by Risk Level



- Patch management was a key theme observed during the internal penetration test
- 960 hosts were missing a patch for at least 90 days
- The oldest missing patch was published in February 2008

Category	Total # of Findings	# of Hosts in this Category	Findings Per Host
Insecure or Misconfigured Services	1,772	534	3.3
Insecure User Account Management	348	191	1.8
Microsoft Patches	711	132	5.4
Third Party Patches	668	132	5.1
Virtualization Patches	328	37	8.9
Weak or Default Passwords	184	534	0.3



# Assessment Results - Password Findings

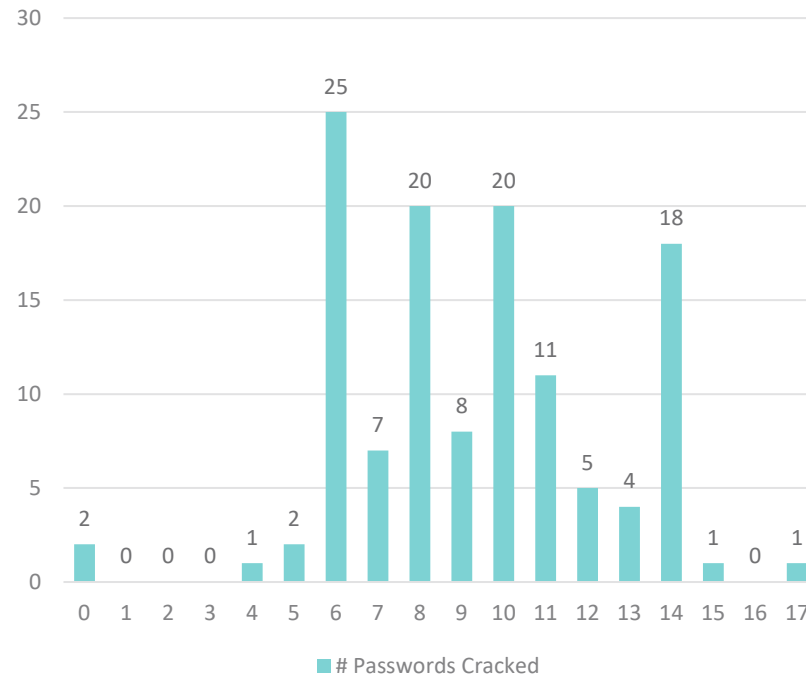
Based on the assessment of the internal environment, the team identified the following vulnerabilities.



## Key Password Observations

- 65% of user passwords were cracked, including 10 privileged accounts
- Default, vendor supplied passwords were observed on numerous enterprise application servers
- Active Directory GPO Settings Observations:
  - Maximum password age is set to 360 days
  - Account lockout duration set to 2 minutes
  - Minimum password length set at 10 characters

### Password Audit Results



Password Audit	Results
Passwords that were all letters	31
Passwords that were all numbers	4
Passwords containing dictionary words	20
Passwords not meeting Windows complexity settings	53



# Assessment Results - Administrator Privileges

During the internal penetration test, the CLA team was able to successfully obtain administrator level privileges within the network.



CLA's attacking computer acted as rogue DHCPv6 server

1



CLA used DHCPv6 and poisoned / hijacked network communication from SAMPLE computers

2



CLA captured the hashed passwords from SAMPLE users on the network and began password cracking

3



Using the compromised accounts, CLA scanned file shares and identified a config file with cleartext database administrator accounts

4



CLA used database credentials to compromise SQL database servers

5



CLA compromised an IT admin account that was logged into the SQL database servers

6



# Assessment Results - Patching and Endpoint Protection

During the internal penetration test, the assessment team observed multiple exploitable weaknesses caused by legacy unsecured communication protocols, as well as a lack of a robust patching and endpoint protections.



## ***Device Hardening***

- Multiple instances of insecure protocols and outdated infrastructure were identified

## ***Microsoft and Third Party Software Patches***

- Over 900 hosts were missing critical patches, many were multiple years out of compliance

## ***Configuration Management***

- Observations included files containing cleartext passwords, domain controller settings, and DHCP settings

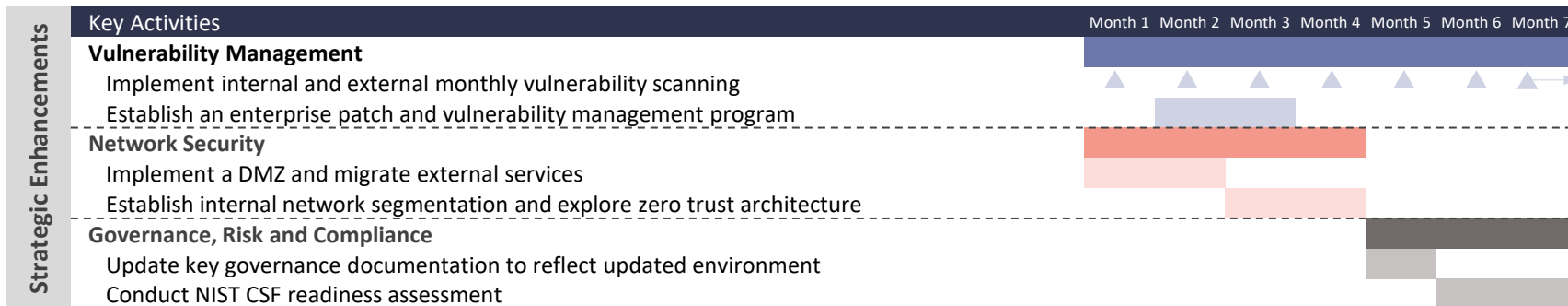
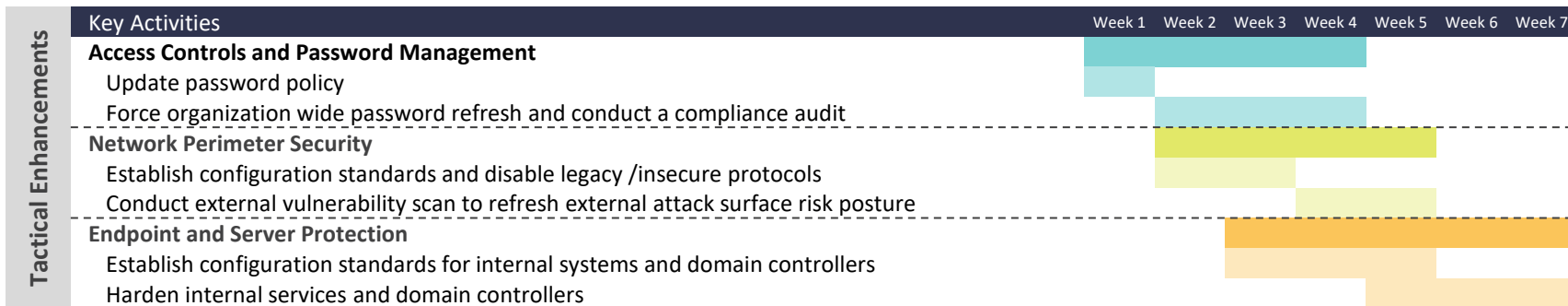
## **Notable Missing Patches**

- ETERNALBLUE\*
- BlueKeep\*
- Rejetto HTTP server
- Log4J Java instances\*

\*Patches known to be exploited by ransomware



# Remediation Recommendations



# Thank you!

Randy Romes  
CISSP, CRISC, CISA, MCP, PCI-QSA  
Principal – Cybersecurity  
612.397.3114  
randy.romes@CLAconnect.com



CLAconnect.com



CPAs | CONSULTANTS | WEALTH ADVISORS

©2025 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAglobal.com/disclaimer](https://www.claglobal.com/disclaimer).  
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



# Closing





# Register Today!

**Navigating Federal Funding  
Uncertainty**

February 27 | 1 – 2 p.m. CT





# *Thank you!*



CLAconnect.com



CPAs | CONSULTANTS | WEALTH ADVISORS

©2025 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAglobal.com/disclaimer](https://www.claglobal.com/disclaimer).  
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.