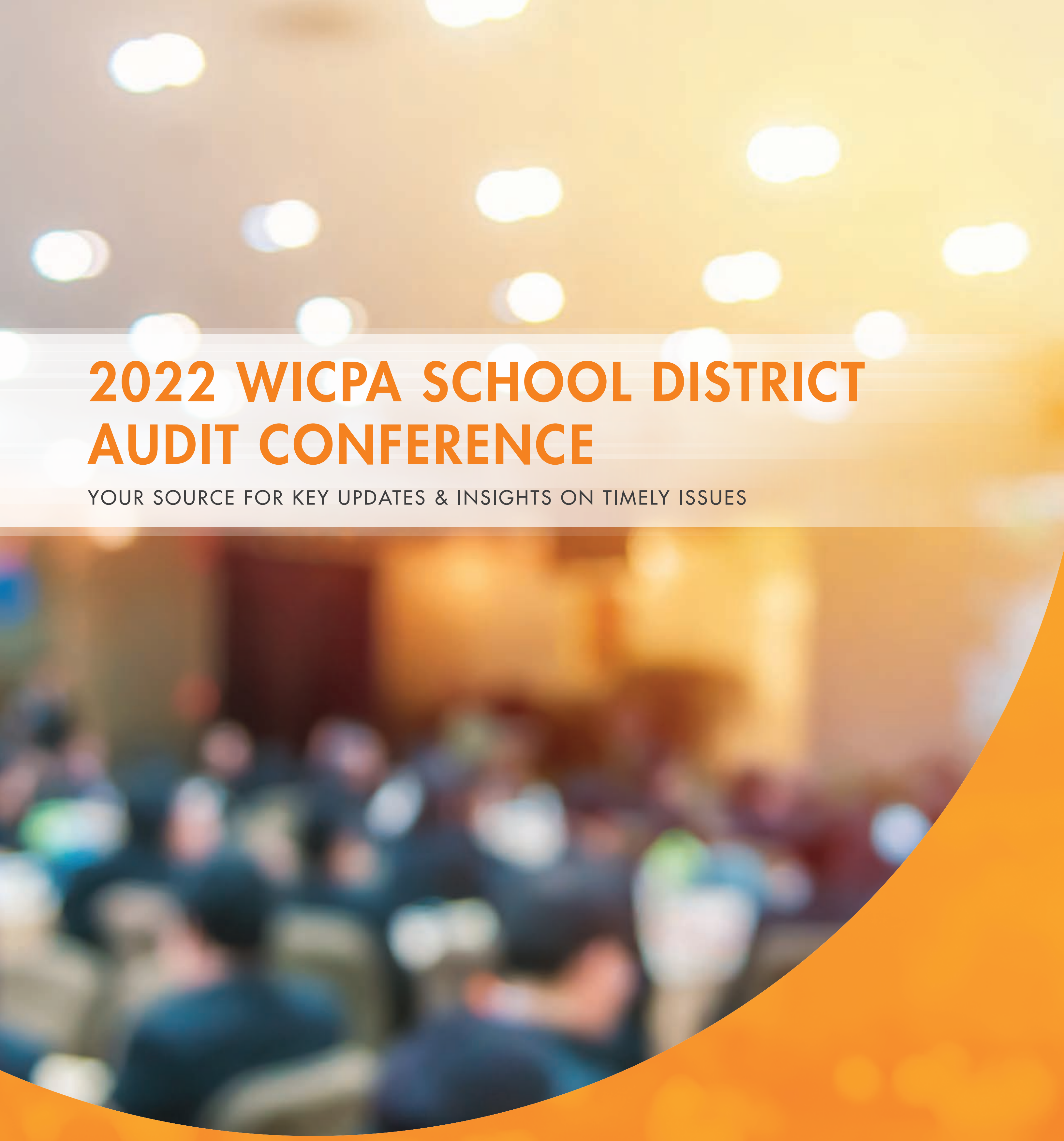


2022 WICPA SCHOOL DISTRICT AUDIT CONFERENCE

YOUR SOURCE FOR KEY UPDATES & INSIGHTS ON TIMELY ISSUES

TUESDAY, MAY 24

KALAHARI RESORT & CONVENTION CENTER
& WICPA CPE LIVESTREAM

2022 WICPA SCHOOL DISTRICT AUDIT CONFERENCE

MATERIALS AT A GLANCE

The following materials are from the morning sessions of the 2022 WICPA School District Audit Conference held on Tuesday, May 24, including:

- DPI Update
- Cybersecurity Threats, Trends & Strategies

UPCOMING WICPA CONFERENCES

YOUR SOURCE FOR KEY UPDATES & INSIGHTS ON TIMELY ISSUES

NETWORK

LEARN

IMPLEMENT

SUCCEED

SAVE THE DATE!

Business & Industry Fall Conference

Tuesday, Sept. 13
Brookfield Conference Center, Brookfield

Wednesday, Oct. 26
Glacier Canyon Lodge, Wisconsin Dells

Not-for-Profit Accounting Conference

Tuesday, Sept. 20
Brookfield Conference Center, Brookfield

Tax Conference

Thursday, Nov. 3 - Friday, Nov. 4
Brookfield Conference Center, Brookfield

Accounting & Auditing Conference

Wednesday, Nov. 16
Brookfield Conference Center, Brookfield

Accounting Technology Conference

Thursday, Dec. 8
Brookfield Conference Center, Brookfield

WISCONSIN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS
WI CPA

WICPA members save up to $150 on registration!
Registration opens approximately eight weeks prior to a conference. View conferences currently open for registration at wicpa.org/conferences.

2022 WICPA GOLF OUTING

FRIDAY, SEPT. 16 – Ironwood Golf Course, Sussex

SCHEDULE

8:30 a.m.
Registration & Breakfast

9:00 a.m.
Practice Greens
& Driving Range

10:00 a.m.
Shotgun Start

144 PERSON LIMIT

4-Person Scramble
$90 per Golfer
$360 for Foursome

HOLE & EVENT PRIZES

$500 Inside the Circle Contest
$500+ in Individual Awards
$500+ in Team Awards

REGISTRATION INCLUDES

18 Holes of Golf With Cart
Practice Greens & Driving Range
Continental Breakfast & Lunch
Beverage Vouchers
Hole & Event Prizes
Entry in the Raffle Drawings
Awards Reception & Appetizers

For more information and to register, visit wicpa.org/GolfOuting**.**

CONNECT

A GREAT WAY FOR WICPA MEMBERS TO COLLABORATE

WICPA Connect is your exclusive members-only networking and knowledge base designed to connect you with WICPA members and resources.

- **Network with peers** and grow your contact list using the member directory of more than 7,000 members.
- **Post questions** to find out from fellow members who have the expertise or may have been in the same situation.
- **Personalize your profile** by adding your interests, education, experience, honors and even your photo.
- **Contribute and download resources** such as documents, whitepapers, articles, reports, guides and more.
- **Share your knowledge and expertise** by answering questions and offering your insights and ideas to fellow members.
- **Customize your experience** with controls for profile visibility, discussion signatures, notifications and more.

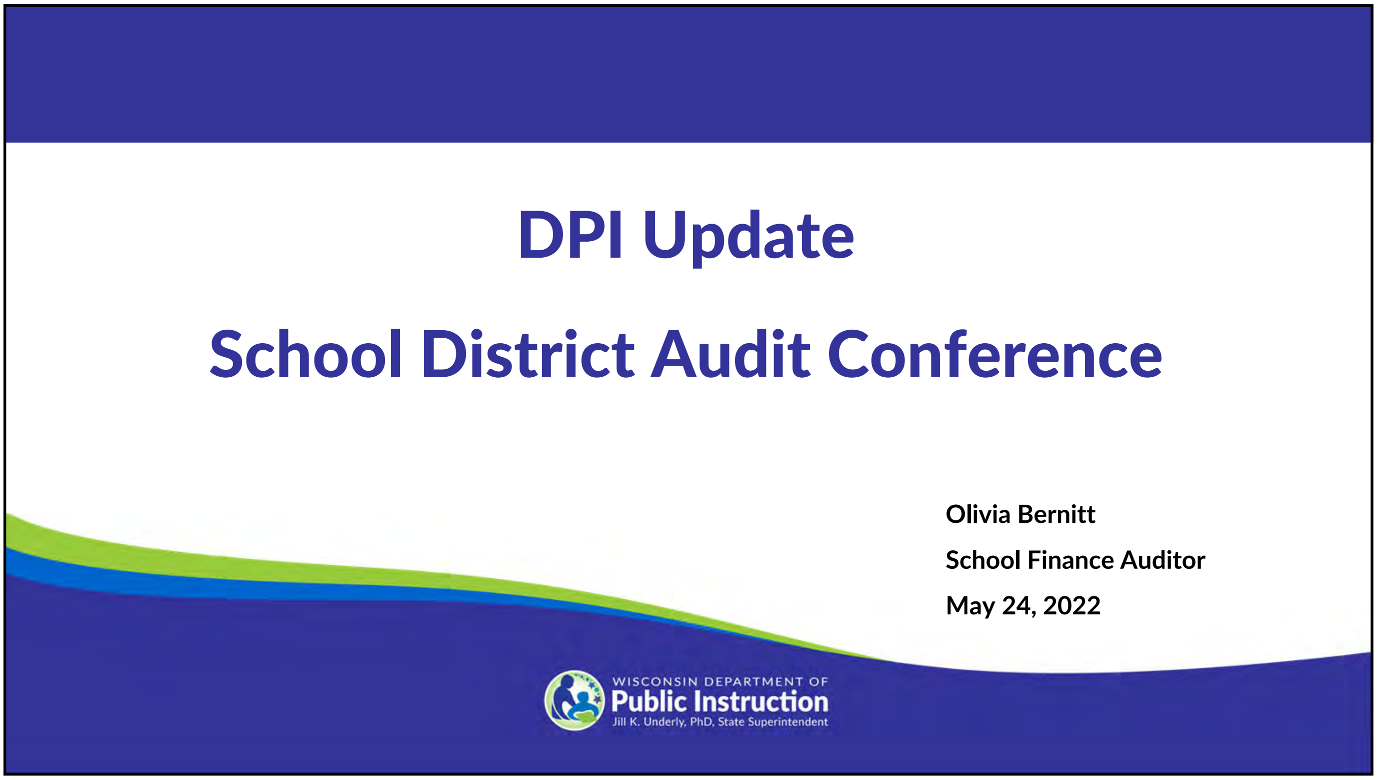
As a WICPA member, you already have a profile on WICPA Connect.
Simply go to wicpa.org/connect and sign in using your existing website login information.

Connect with thousands of fellow members now at **wicpa.org/connect**

8:10 – 9:35 a.m.

DPI Update

Olivia Bernitt, *School Finance Auditor, Wisconsin Department of Public Instruction*



DPI Update

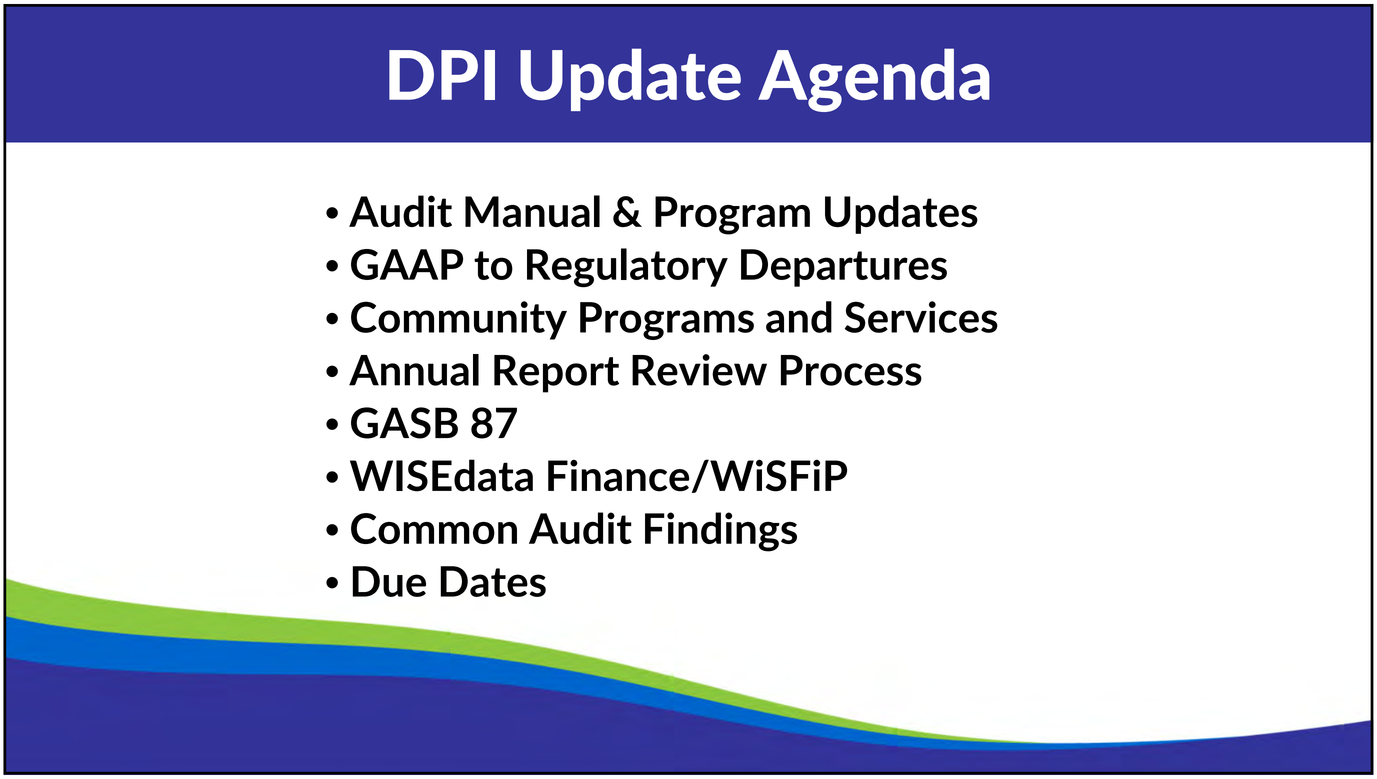
School District Audit Conference

Olivia Bernitt

School Finance Auditor

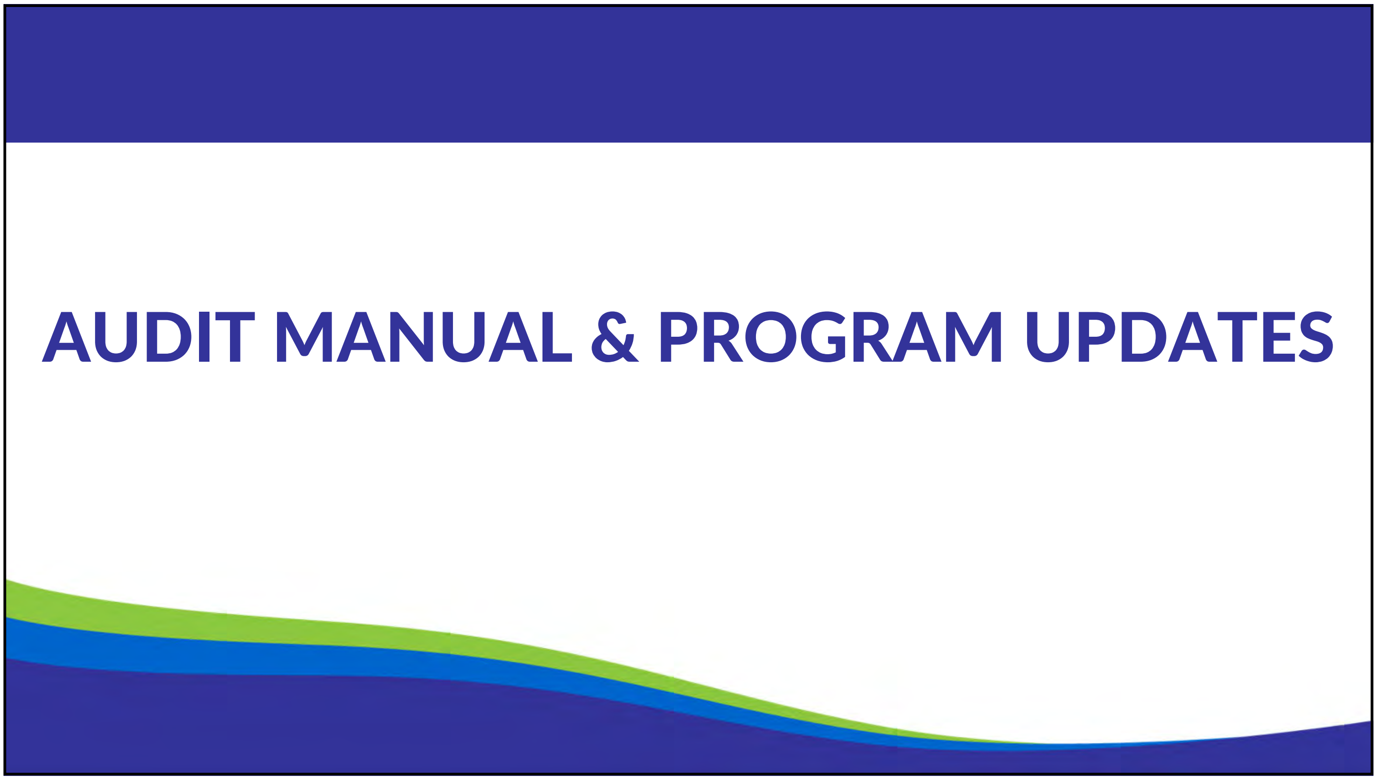
May 24, 2022

WISCONSIN DEPARTMENT OF
Public Instruction
Jill K. Underly, PhD, State Superintendent

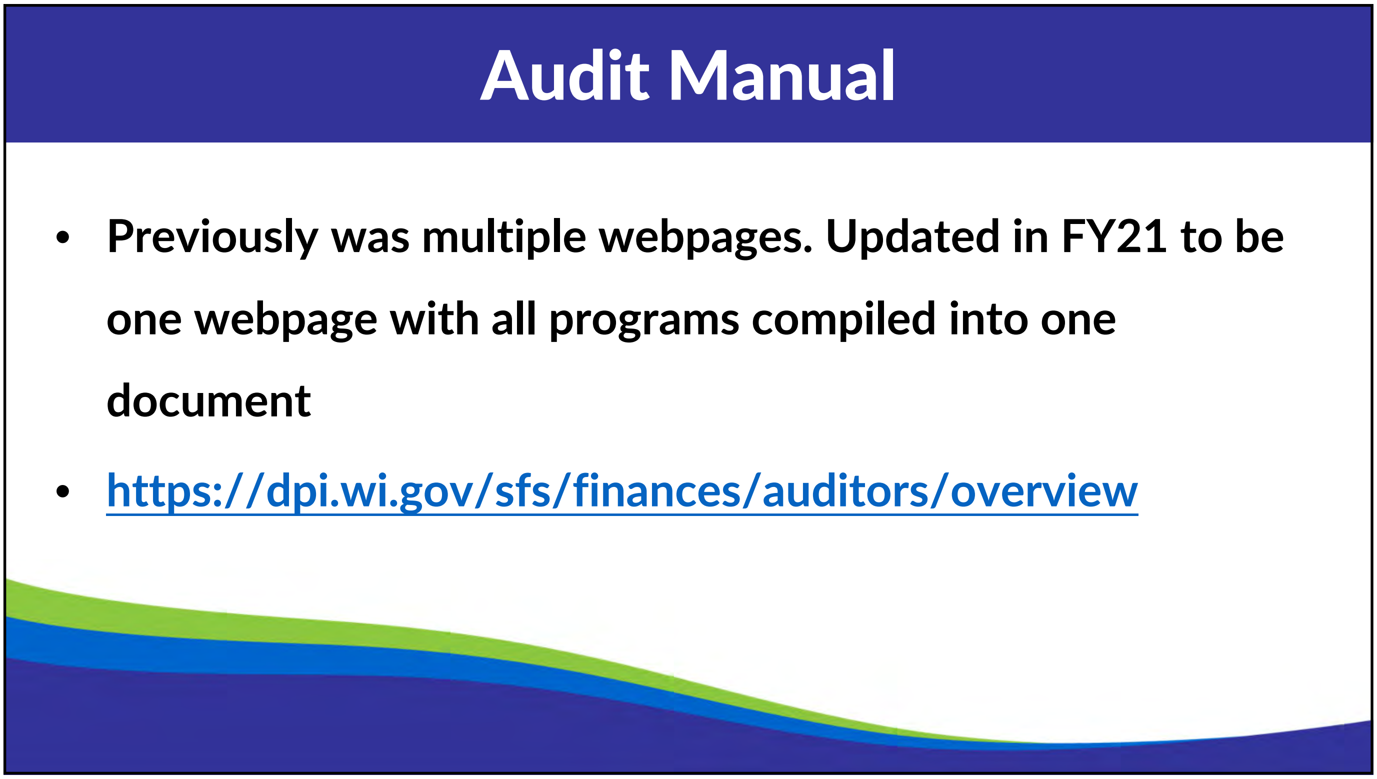


DPI Update Agenda

- Audit Manual & Program Updates
- GAAP to Regulatory Departures
- Community Programs and Services
- Annual Report Review Process
- GASB 87
- WISEdata Finance/WiSFiP
- Common Audit Findings
- Due Dates

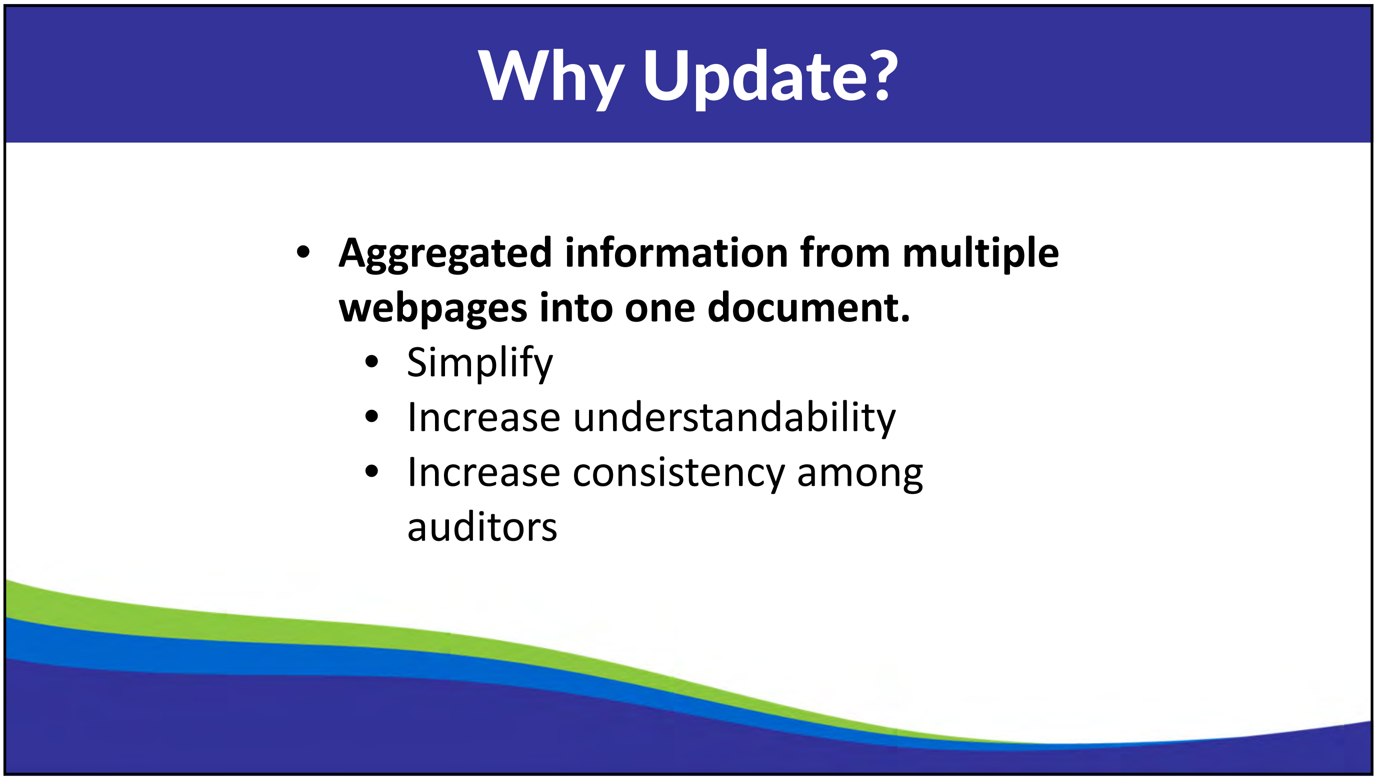


AUDIT MANUAL & PROGRAM UPDATES



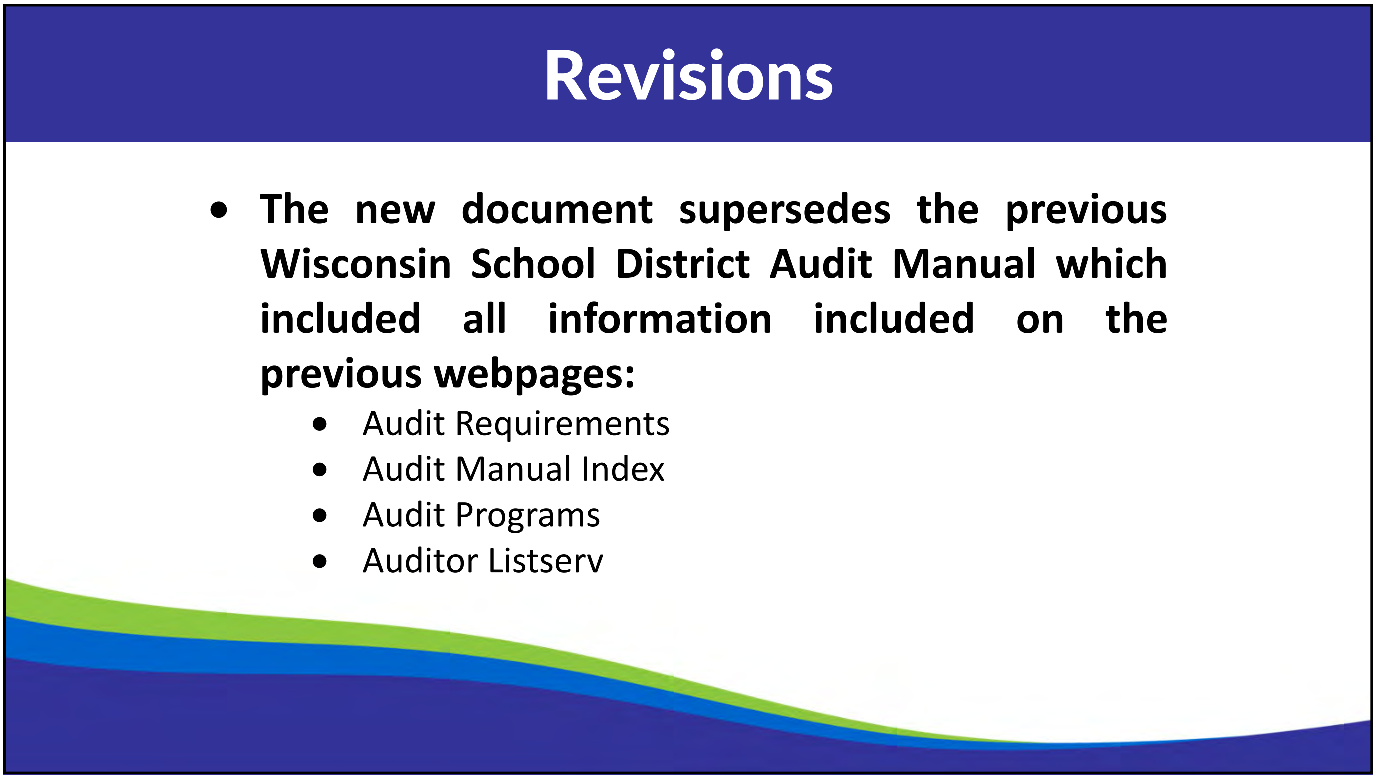
Audit Manual

- Previously was multiple webpages. Updated in FY21 to be one webpage with all programs compiled into one document
- https://dpi.wi.gov/sfs/finances/auditors/overview



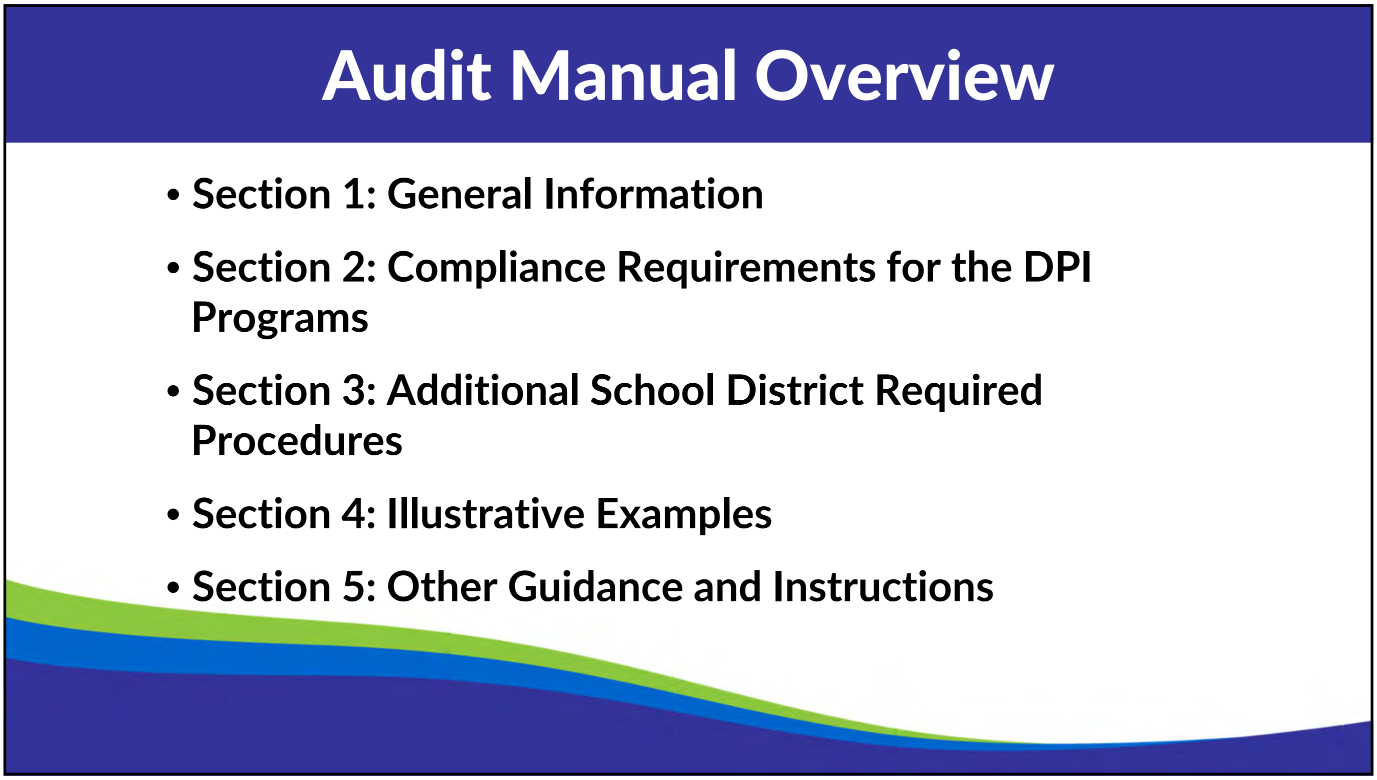
Why Update?

- **Aggregated information from multiple webpages into one document.**
  - Simplify
  - Increase understandability
  - Increase consistency among auditors



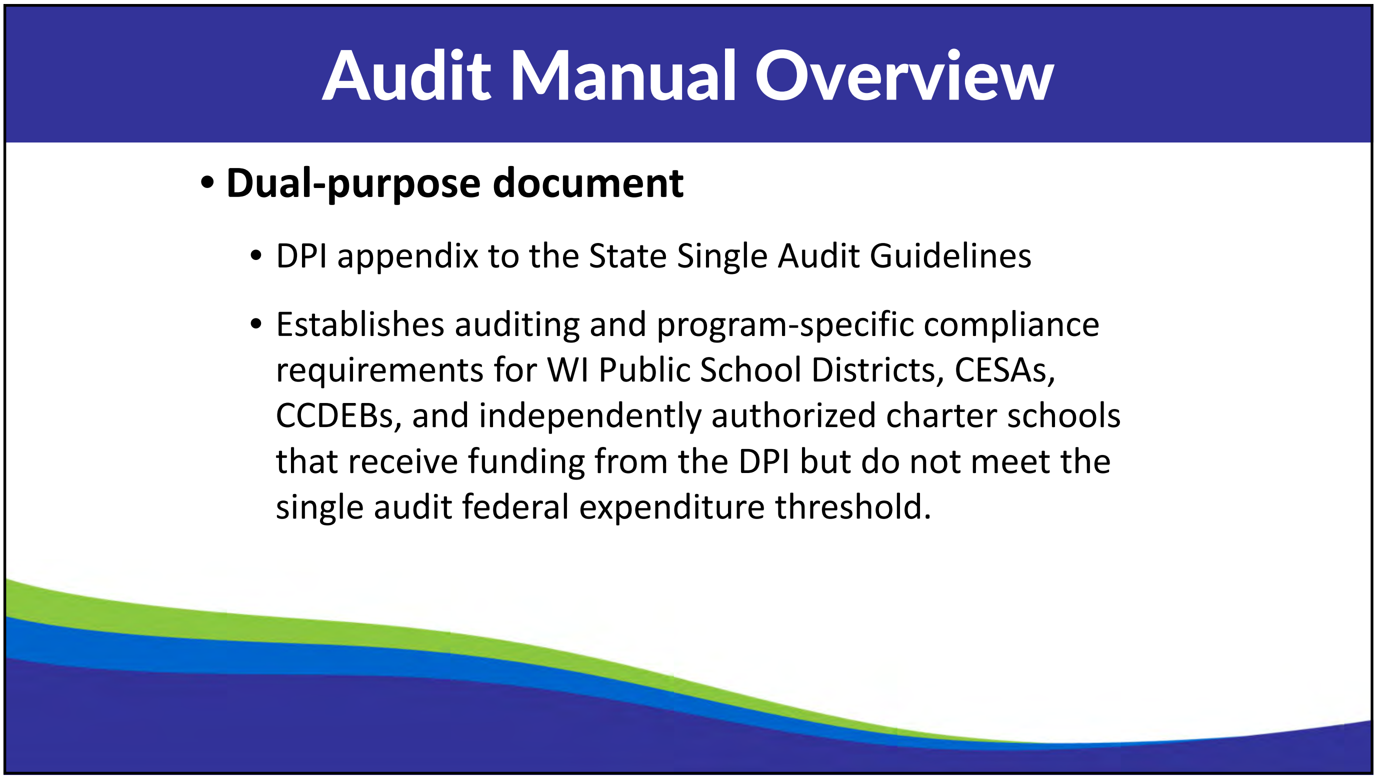
Revisions

- **The new document supersedes the previous Wisconsin School District Audit Manual which included all information included on the previous webpages:**
  - Audit Requirements
  - Audit Manual Index
  - Audit Programs
  - Auditor Listserv



Audit Manual Overview

- Section 1: General Information
- Section 2: Compliance Requirements for the DPI Programs
- Section 3: Additional School District Required Procedures
- Section 4: Illustrative Examples
- Section 5: Other Guidance and Instructions



Audit Manual Overview

- **Dual-purpose document**
  - DPI appendix to the State Single Audit Guidelines
  - Establishes auditing and program-specific compliance requirements for WI Public School Districts, CESAs, CCDEBs, and independently authorized charter schools that receive funding from the DPI but do not meet the single audit federal expenditure threshold.

Updates – State Major Program Determination

- **Audits in accordance with SSAG**
  - Risk-based approach outlined in SSAG Section 3.4 applied to all state funding to identify state major programs.
- **Audits in accordance with WI School District Audit Manual**
  - Risk-based approach outlined in SSAG Section 3.4 should be applied to the DPI funding to identify state major programs.

SSAG Main Doc, Section 3.4

- **The auditor shall apply the risk-based approach from the Uniform Guidance to identify which programs will be tested as state major programs, with the following modifications:**
  - Consider prior audit experience with state programs when assessing whether the auditee is a low-risk agency for purposes of the percentage-of-coverage rule for state programs.
  - The threshold for Type A programs is $250,000.
  - The threshold for Type B programs is $62,500.

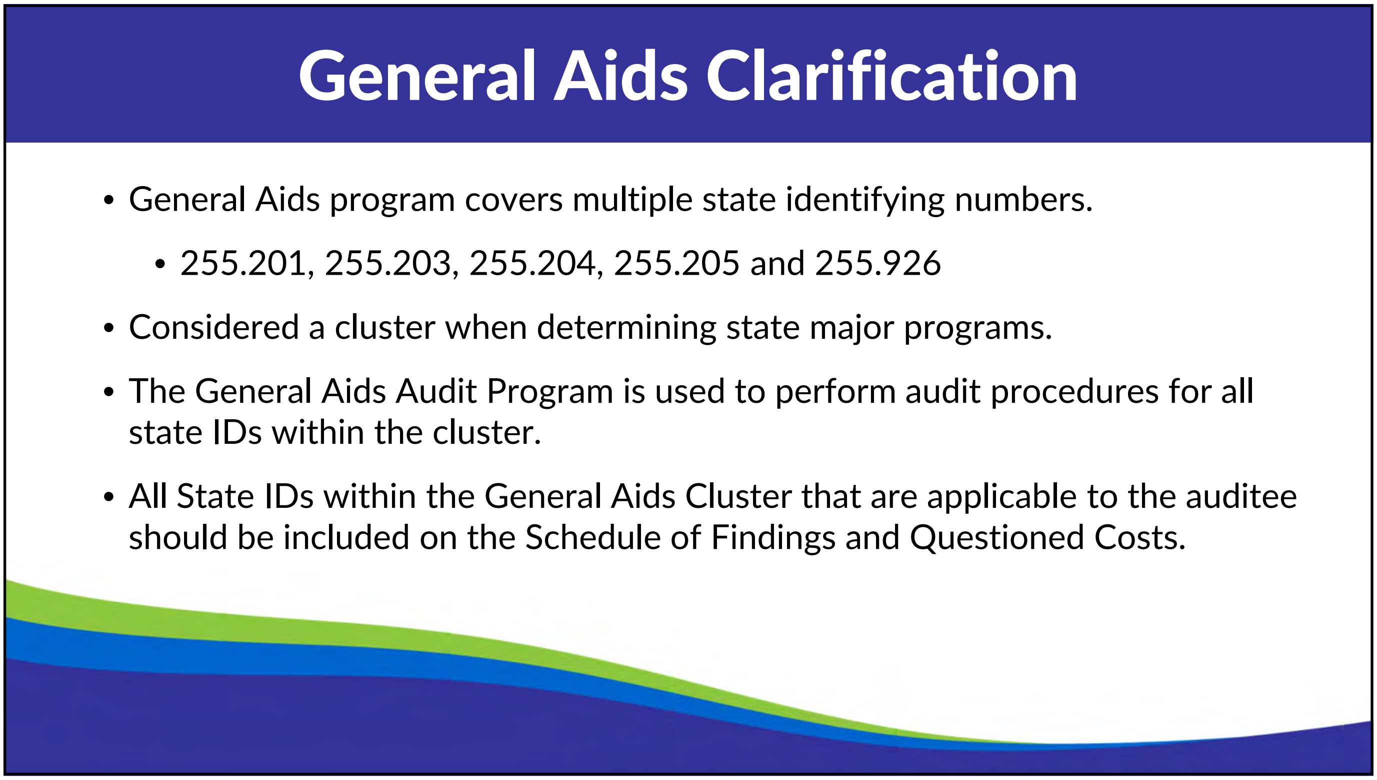
SSAG Main Doc, Section 3.4

- **. . . with the following modifications:**
  - The agency may designate state or federal pass-through programs to be automatically considered to be Type A state programs, and these programs are tested as state major unless the auditor assesses them to be low-risk, but at least once every three years. In addition, granting agencies may designate programs to be state major, so that these programs are always tested when the auditee has the programs. Programs that are state funded that had less than $25,000 in expenditures should not be treated as state major programs unless they are needed to satisfy the percent-of-coverage threshold for state programs.

SSAG Main Doc, Section 3.4

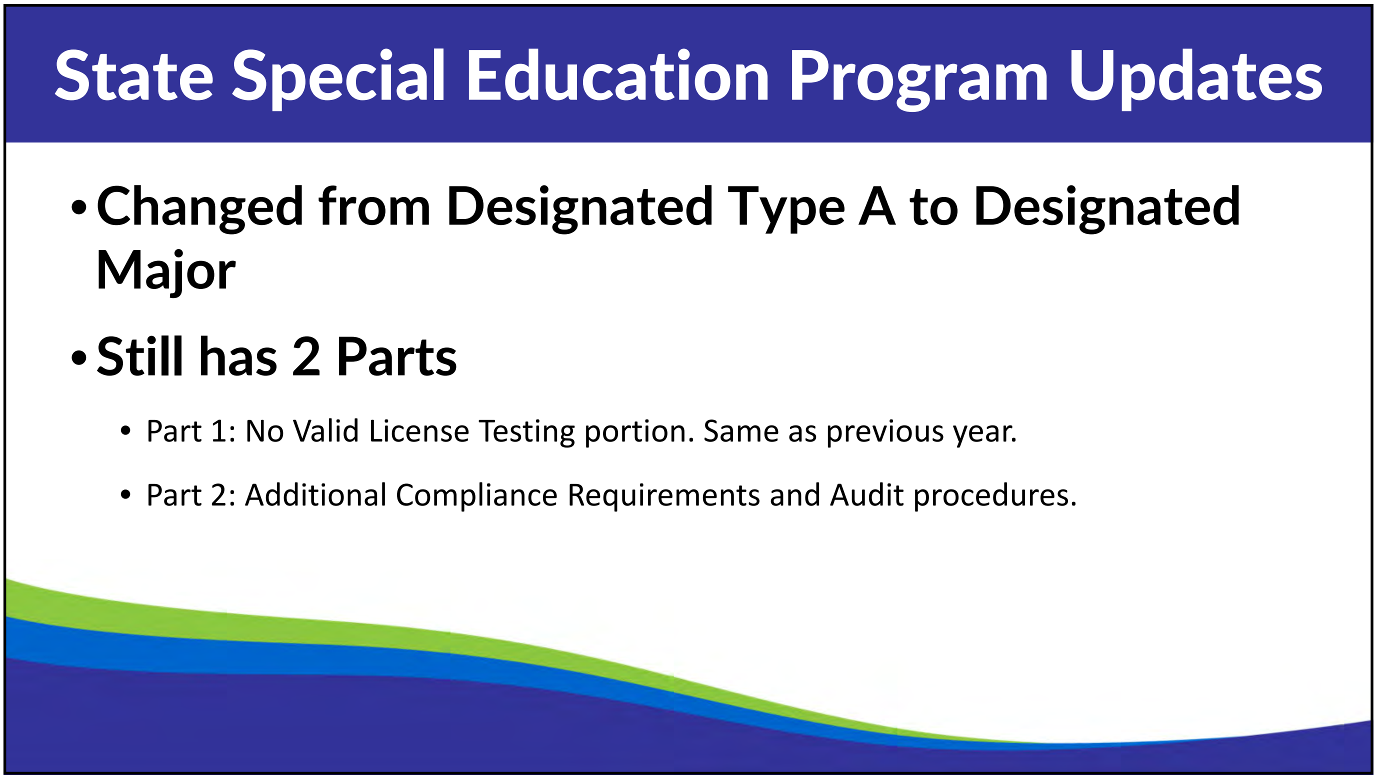
- **. . . with the following modifications:**
  - Workpaper documentation should include, for each program: the name of the program, the amounts of expenditures, whether the program is Type A or Type B, the factors considered in the risk assessment, the auditor’s assessment of the risk for each factor, and the overall assessment of risk. The workpapers should also show how risk is reflected in the testing for high-risk programs.

  - For a low-risk agency, if current year significant deficiencies, material weaknesses, or material noncompliance indicates the potential for a system-wide problem, the auditor needs to expand testing to cover 40% of state program expenditures, i.e. no longer consider the agency to be low risk.



General Aids Clarification

- General Aids program covers multiple state identifying numbers.
  - 255.201, 255.203, 255.204, 255.205 and 255.926
- Considered a cluster when determining state major programs.
- The General Aids Audit Program is used to perform audit procedures for all state IDs within the cluster.
- All State IDs within the General Aids Cluster that are applicable to the auditee should be included on the Schedule of Findings and Questioned Costs.



State Special Education Program Updates

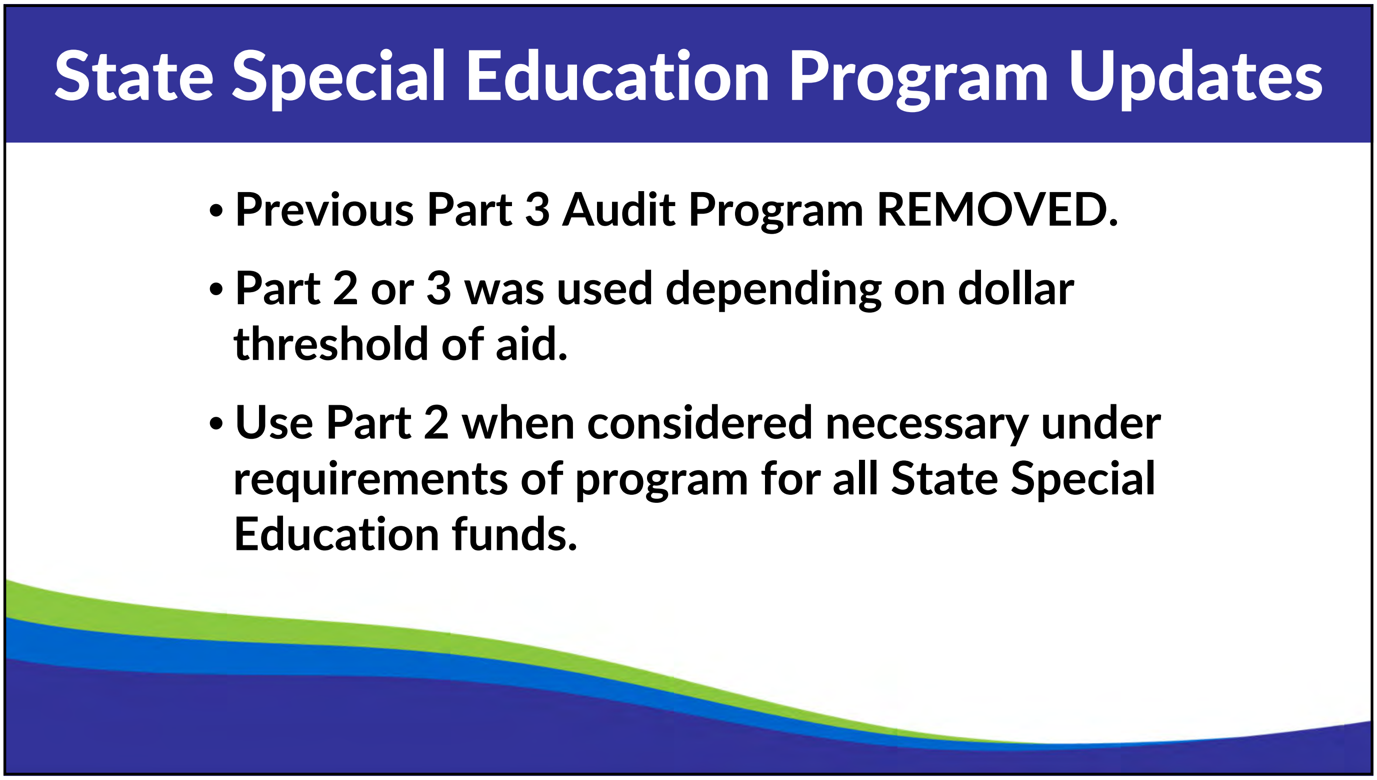
- **Changed from Designated Type A to Designated Major**
- **Still has 2 Parts**
  - Part 1: No Valid License Testing portion. Same as previous year.
  - Part 2: Additional Compliance Requirements and Audit procedures.

State Special Education Program Updates

- **Part 1: Required every year State Special Education is determined to be Major.**
  - Every year, as DPI has designated the program major.
- **Part 2: Required at least once every three years and/or when the program is not considered low-risk.**
  - A risk assessment of the program must be completed every year to determine if Part 2 Compliance requirements are required.

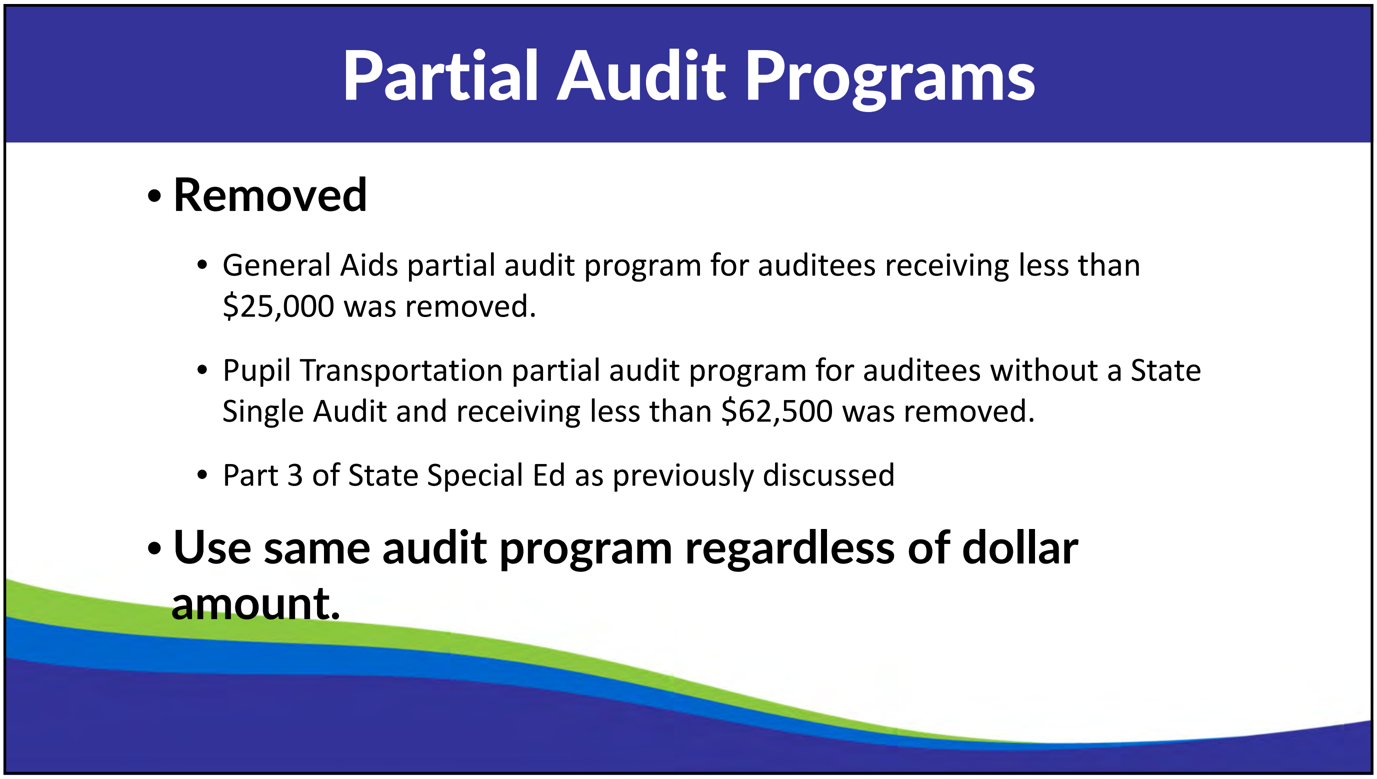
State Special Education Program Updates

- **Background Section of audit program includes a risk assessment that may be used to determine and document when Part 2 needs to be completed.**
  - Uses risk assessment based on Uniform Grant Guidance Type A program risk assessment.



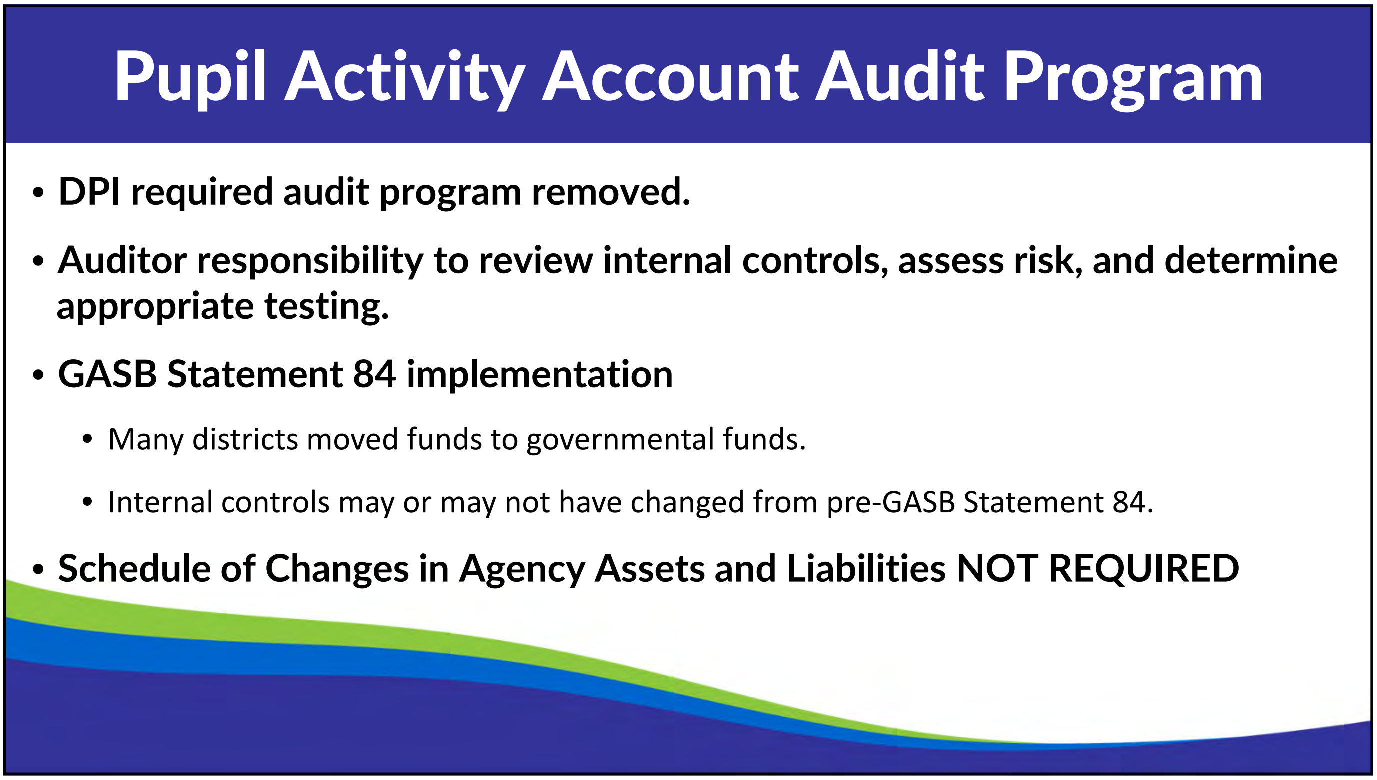
State Special Education Program Updates

- Previous Part 3 Audit Program REMOVED.
- Part 2 or 3 was used depending on dollar threshold of aid.
- Use Part 2 when considered necessary under requirements of program for all State Special Education funds.



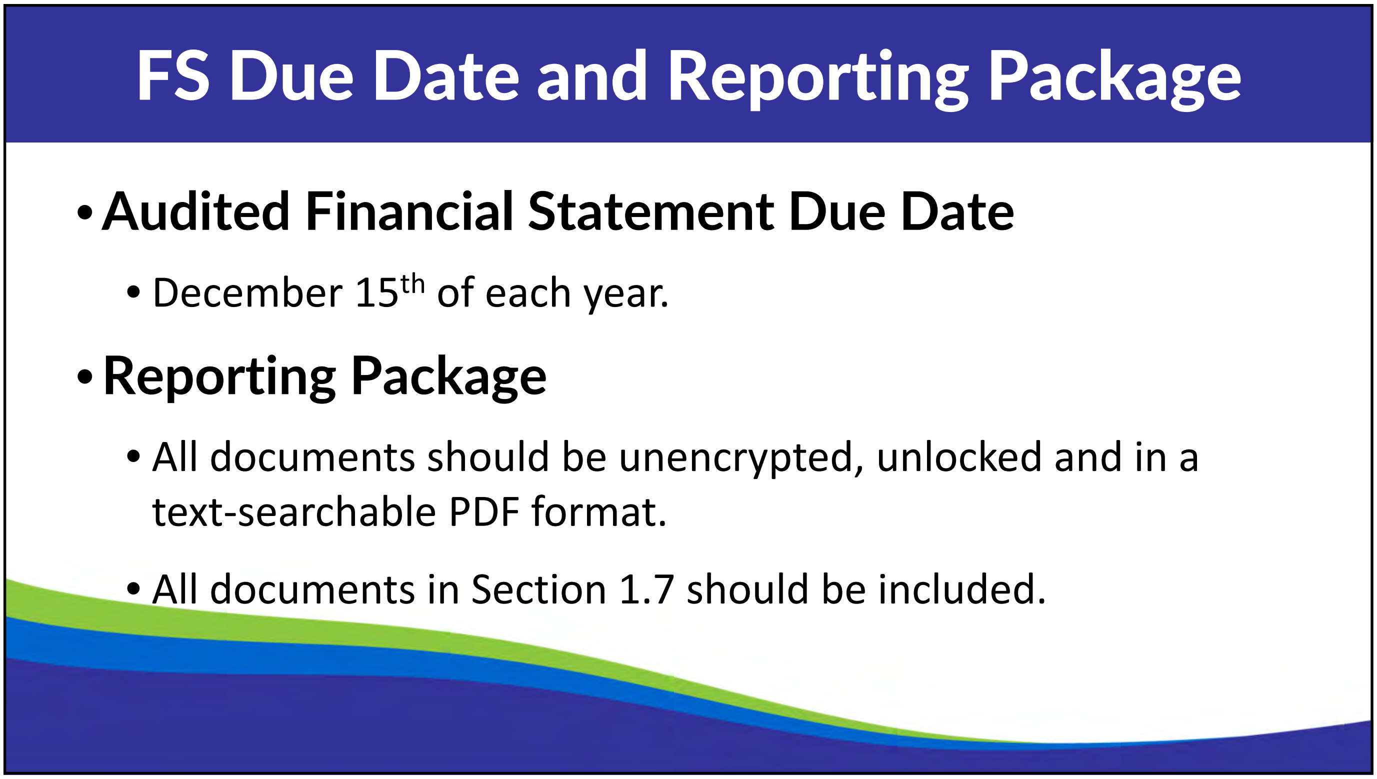
Partial Audit Programs

- Removed
  - General Aids partial audit program for auditees receiving less than $25,000 was removed.
  - Pupil Transportation partial audit program for auditees without a State Single Audit and receiving less than $62,500 was removed.
  - Part 3 of State Special Ed as previously discussed
- Use same audit program regardless of dollar amount.



Pupil Activity Account Audit Program

- **DPI required audit program removed.**
- **Auditor responsibility to review internal controls, assess risk, and determine appropriate testing.**
- **GASB Statement 84 implementation**
  - Many districts moved funds to governmental funds.
  - Internal controls may or may not have changed from pre-GASB Statement 84.
- **Schedule of Changes in Agency Assets and Liabilities NOT REQUIRED**



FS Due Date and Reporting Package

- Audited Financial Statement Due Date
  - December 15th of each year.
- Reporting Package
  - All documents should be unencrypted, unlocked and in a text-searchable PDF format.
  - All documents in Section 1.7 should be included.

Items to Clarify/Update in the Wisconsin School District Audit Manual?

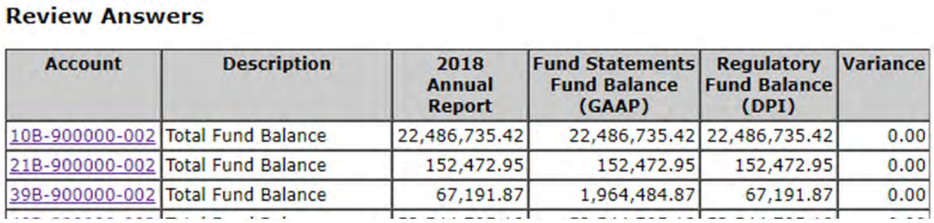
GAAP TO REGULATORY DEPARTURES

GAAP to Regulatory Departures

- Auditor submits PI-1506-AC and PI-1506-FB no later than the last Friday before September 15th.
- District submits the PI-1505 no later than the following Friday.
- These three reports must match.

GAAP to Regulatory Departures

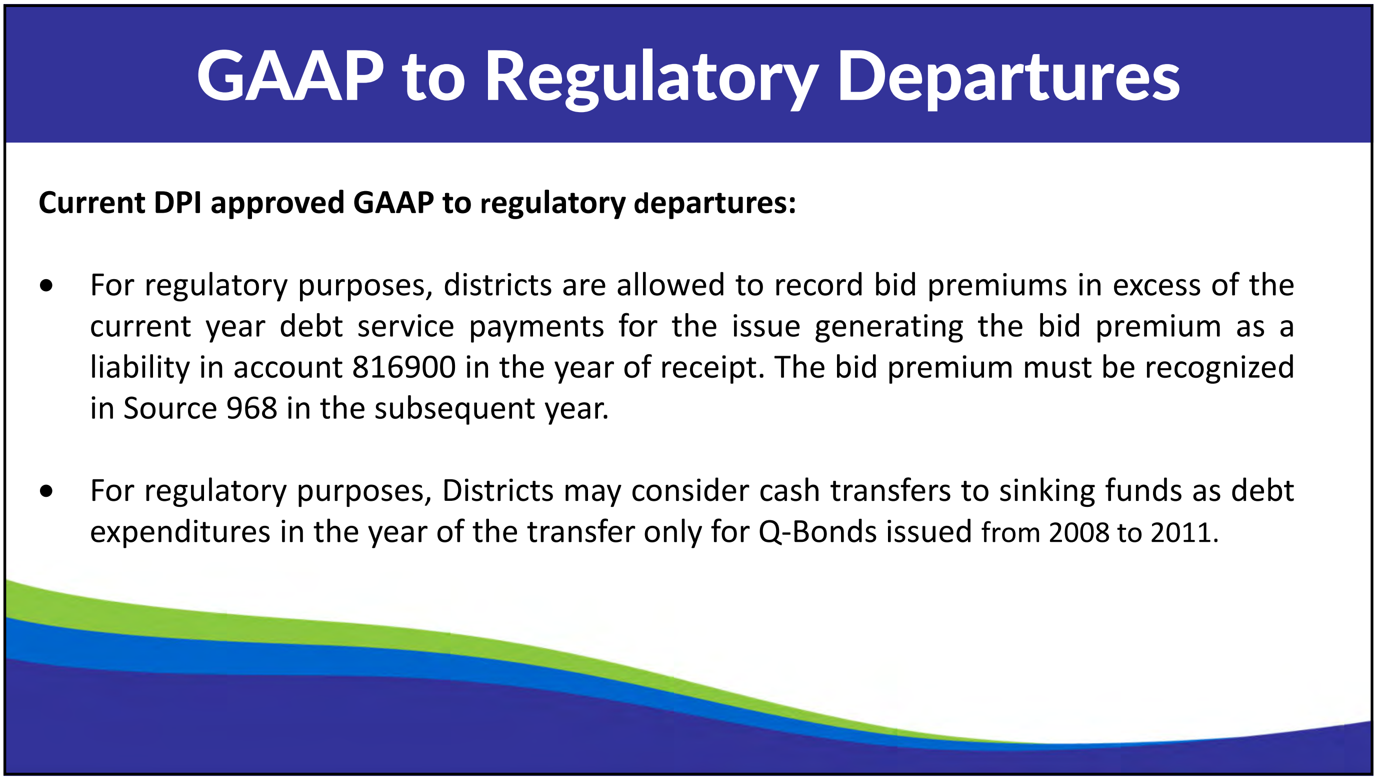
- The DPI reports should be in accordance with modified accrual GAAP except for DPI specified regulatory departures.
- Expect the PI-1506-FB to show GAAP to regulatory departure.



Review Answers

Account	Description	2018 Annual Report	Fund Statements Fund Balance (GAAP)	Regulatory Fund Balance (DPI)	Variance
10B-900000-002	Total Fund Balance	22,486,735.42	22,486,735.42	22,486,735.42	0.00
21B-900000-002	Total Fund Balance	152,472.95	152,472.95	152,472.95	0.00
39B-900000-002	Total Fund Balance	67,191.87	1,964,484.87	67,191.87	0.00

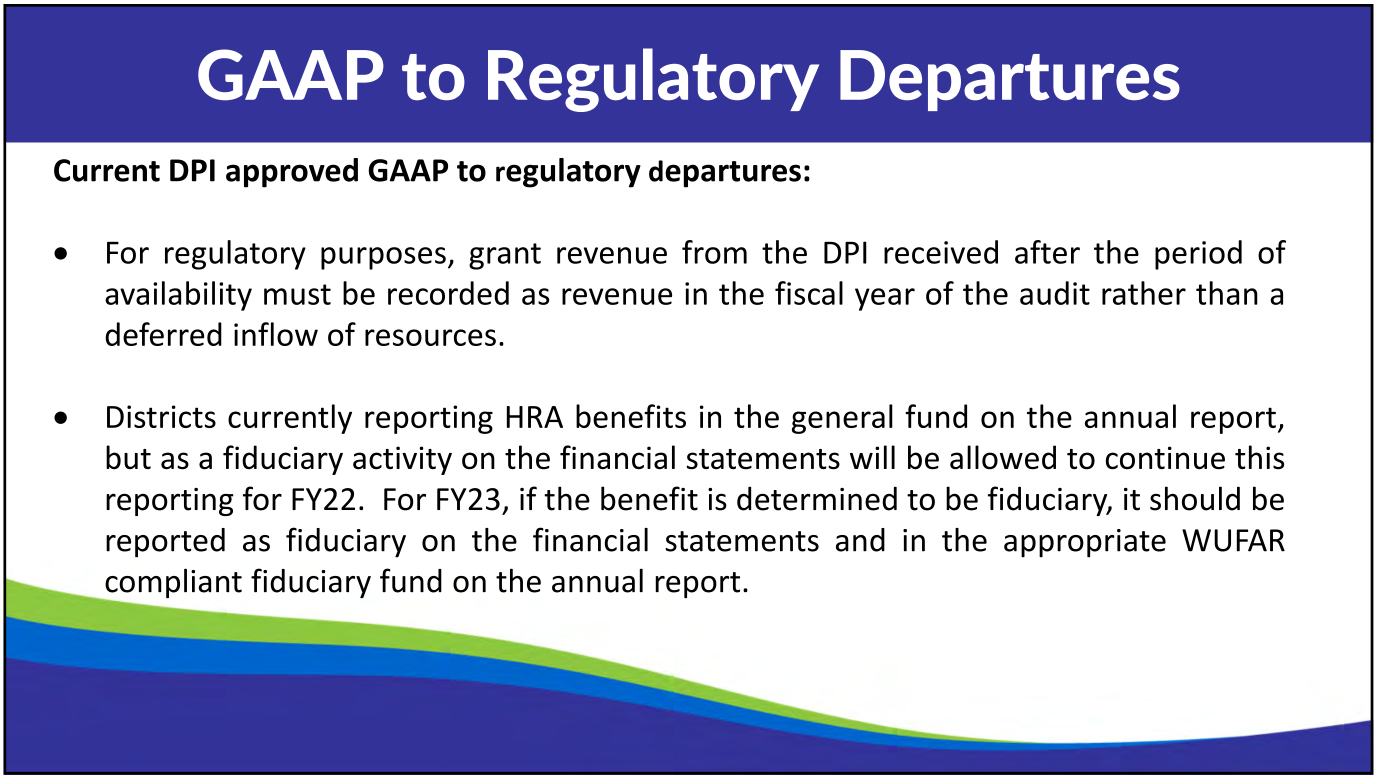
- PI-1506-AC also reports the regulatory balances as it must tie to the District's PI-1505.



GAAP to Regulatory Departures

Current DPI approved GAAP to regulatory departures:

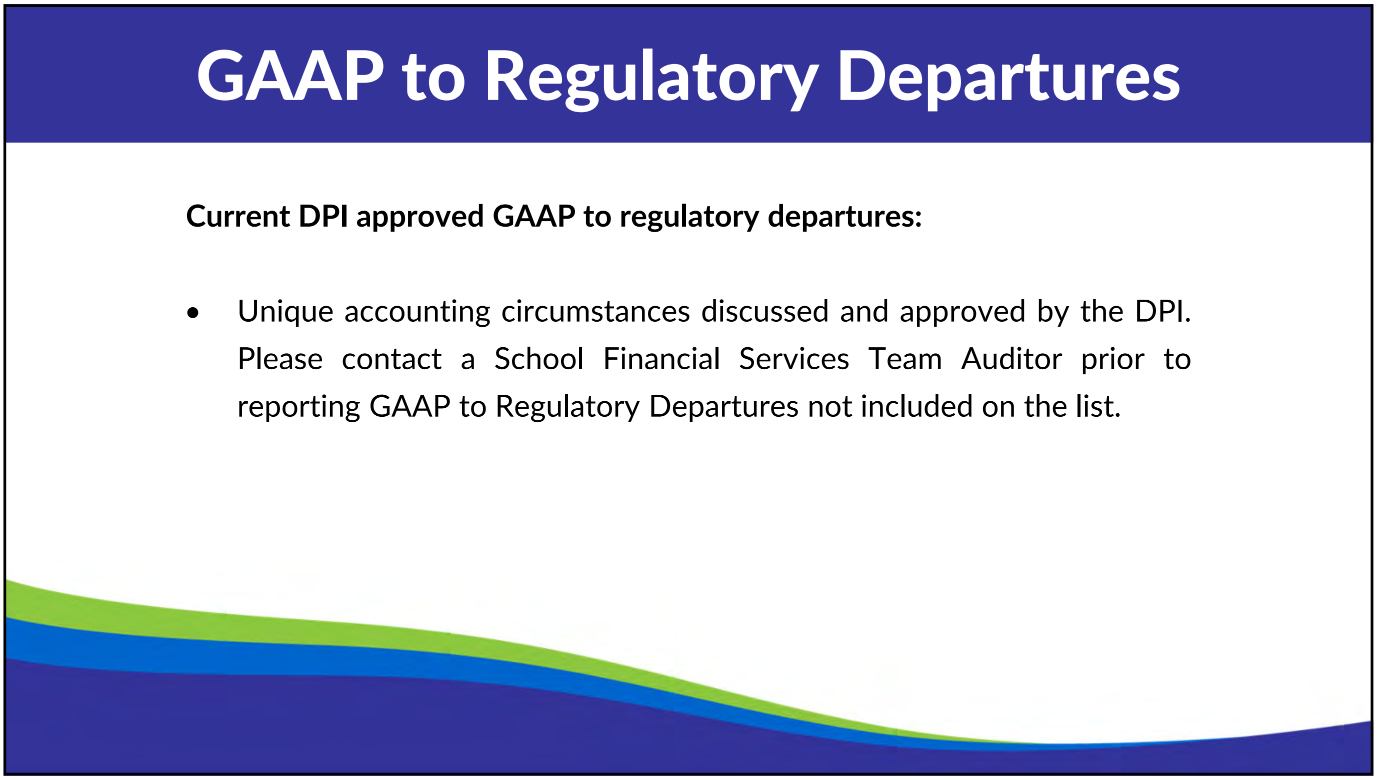
- For regulatory purposes, districts are allowed to record bid premiums in excess of the current year debt service payments for the issue generating the bid premium as a liability in account 816900 in the year of receipt. The bid premium must be recognized in Source 968 in the subsequent year.
- For regulatory purposes, Districts may consider cash transfers to sinking funds as debt expenditures in the year of the transfer only for Q-Bonds issued from 2008 to 2011.



GAAP to Regulatory Departures

Current DPI approved GAAP to regulatory departures:

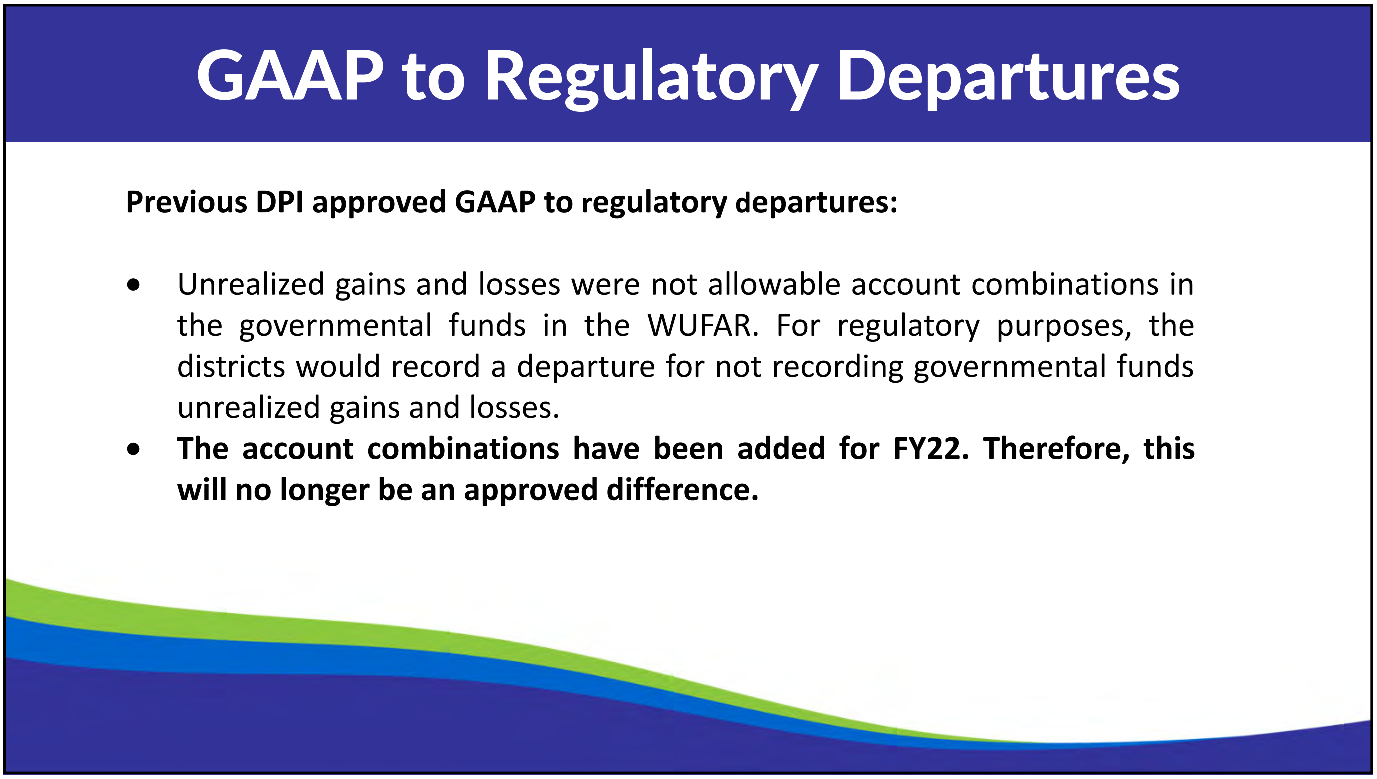
- For regulatory purposes, grant revenue from the DPI received after the period of availability must be recorded as revenue in the fiscal year of the audit rather than a deferred inflow of resources.
- Districts currently reporting HRA benefits in the general fund on the annual report, but as a fiduciary activity on the financial statements will be allowed to continue this reporting for FY22. For FY23, if the benefit is determined to be fiduciary, it should be reported as fiduciary on the financial statements and in the appropriate WUFAR compliant fiduciary fund on the annual report.



GAAP to Regulatory Departures

Current DPI approved GAAP to regulatory departures:

- Unique accounting circumstances discussed and approved by the DPI. Please contact a School Financial Services Team Auditor prior to reporting GAAP to Regulatory Departures not included on the list.



GAAP to Regulatory Departures

Previous DPI approved GAAP to regulatory departures:

- Unrealized gains and losses were not allowable account combinations in the governmental funds in the WUFAR. For regulatory purposes, the districts would record a departure for not recording governmental funds unrealized gains and losses.
- **The account combinations have been added for FY22. Therefore, this will no longer be an approved difference.**

COMMUNITY PROGRAMS AND SERVICES

Community Programs and Services

- Each function, program or service operated by a school district is a part of the district's general school operations (normally Fund 10 costs)

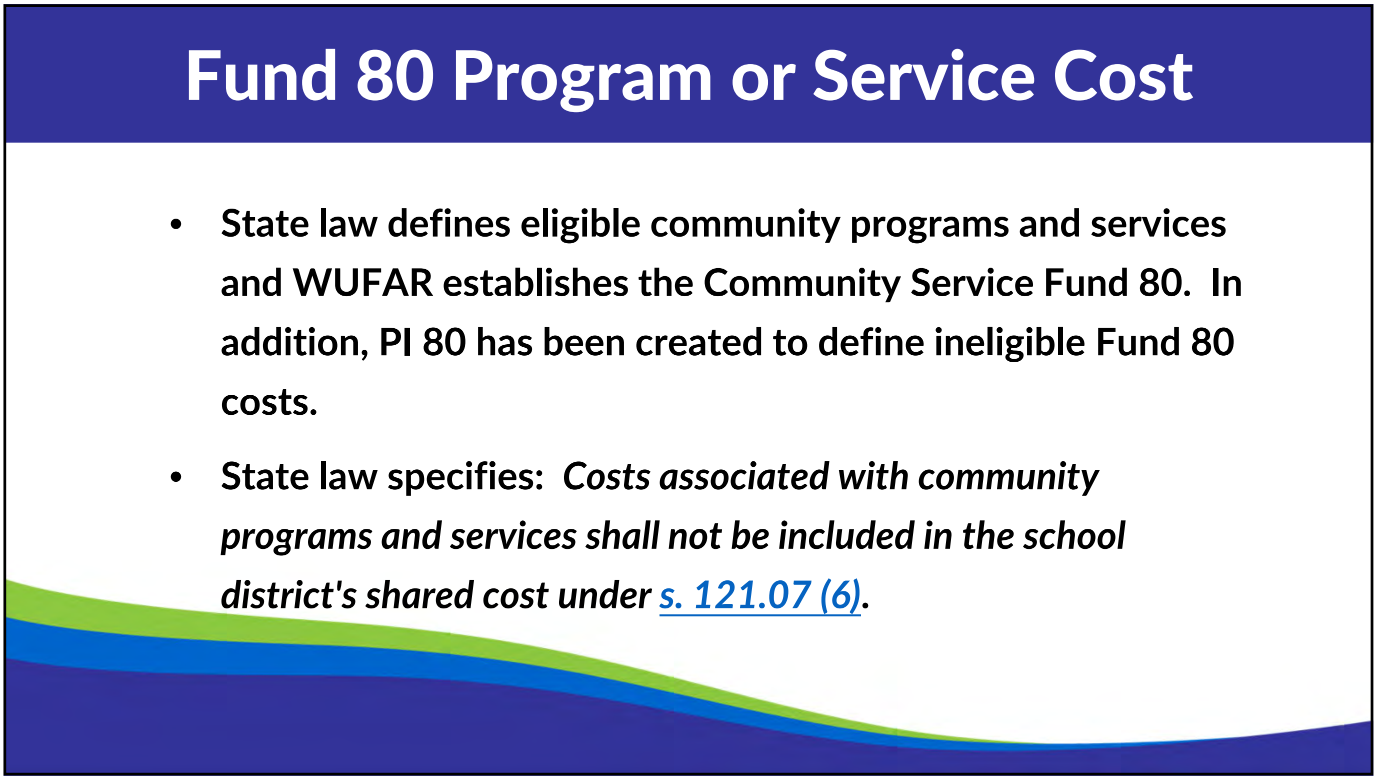
➢**Unless documented** to be part of the school board's established community programs or services offered under Wis. Stat. 120.13(19)

Community Service Fund Information

Fund 80 Overview

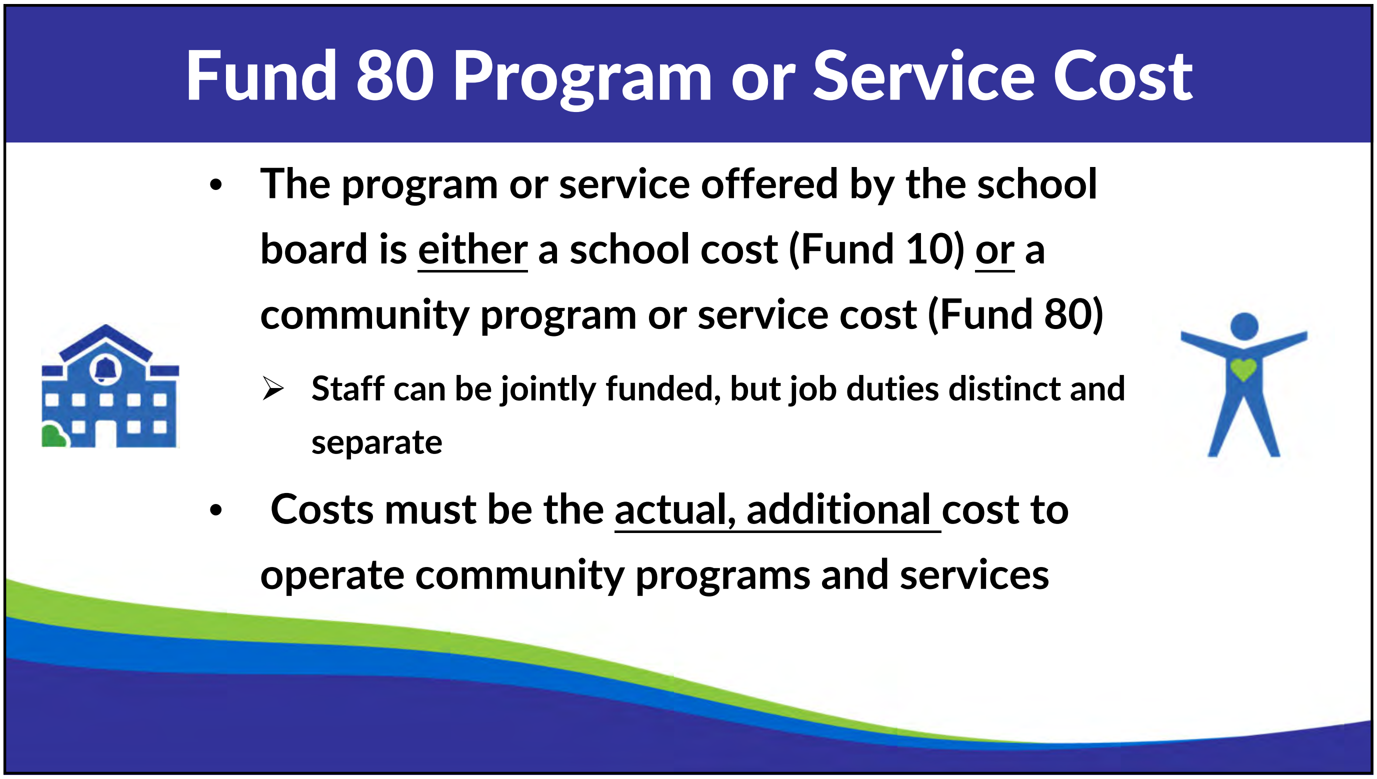
The Community Program and Services (CPS) F
account for activities such as adult education,
programs such as evening swimming pool op
leagues, elderly food service programs, non-s
preschool, day care services and other progra
elementary and secondary educational progr

https://dpi.wi.gov/sfs/finances/fund-info/community-service/overview



Fund 80 Program or Service Cost

- State law defines eligible community programs and services and WUFAR establishes the Community Service Fund 80. In addition, PI 80 has been created to define ineligible Fund 80 costs.
- State law specifies: *Costs associated with community programs and services shall not be included in the school district's shared cost under s. 121.07 (6)*.

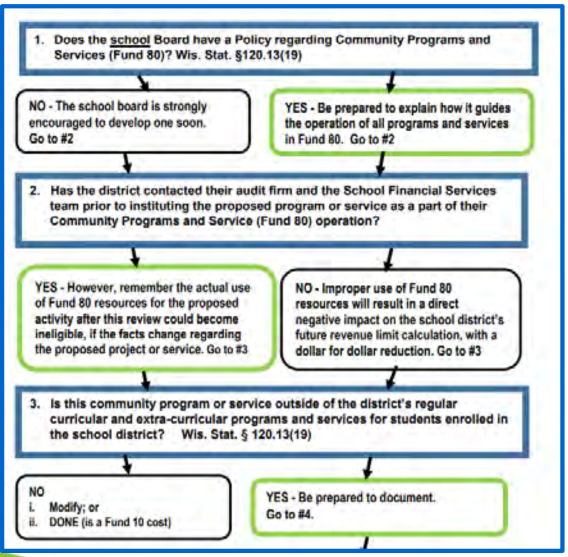


Fund 80 Program or Service Cost

- The program or service offered by the school board is either a school cost (Fund 10) or a community program or service cost (Fund 80)
  - ➢ Staff can be jointly funded, but job duties distinct and separate
- Costs must be the actual, additional cost to operate community programs and services

Decision Tree for Community Programs

- Tool to ask and answer 10 questions when reviewing community programs and services expenditures eligibility
- https://dpi.wi.gov/sites/default/files/imce/sfs/pdf/Final-Decision-Tree-for-Potential-Fund-80-03-2019.pdf



1. Does the school Board have a Policy regarding Community Programs and Services (Fund 80)? Wis. Stat. §120.13(19)

NO - The school board is strongly encouraged to develop one soon. Go to #2

YES - Be prepared to explain how it guides the operation of all programs and services in Fund 80. Go to #2

2. Has the district contacted their audit firm and the School Financial Services team prior to instituting the proposed program or service as a part of their Community Programs and Service (Fund 80) operation?

YES - However, remember the actual use of Fund 80 resources for the proposed activity after this review could become ineligible, if the facts change regarding the proposed project or service. Go to #3

NO - Improper use of Fund 80 resources will result in a direct negative impact on the school district's future revenue limit calculation, with a dollar for dollar reduction. Go to #3

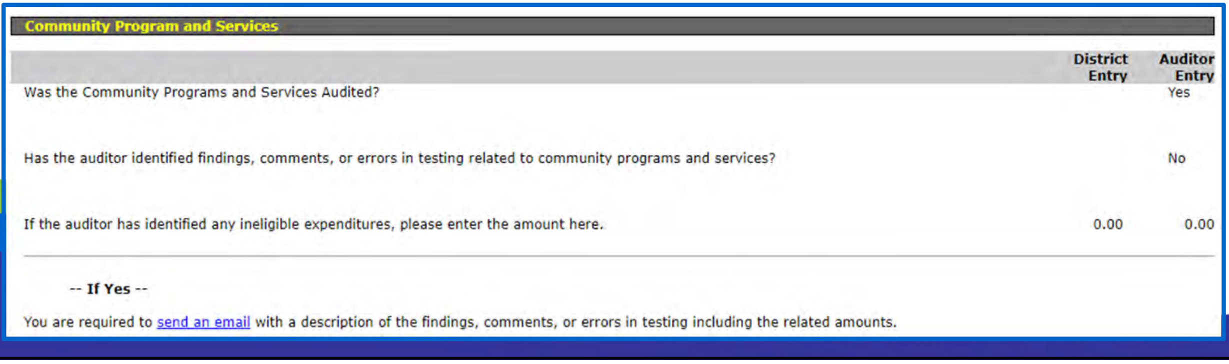
3. Is this community program or service outside of the district's regular curricular and extra-curricular programs and services for students enrolled in the school district? Wis. Stat. § 120.13(19)

NO
i. Modify; or
ii. DONE (is a Fund 10 cost)

YES - Be prepared to document. Go to #4.

Reporting Ineligible F80 Costs

- Report ineligible expenditures identified by the auditor on the PI-1506-AC
- Do not report expenditures that have been reclassified prior to filing the PI-1506-AC
- Report ineligible expenditures identified on the PI-1506-AC in the Schedule of Findings and Questioned Costs in the Financial Statements



Community Program and Services

	District Entry	Auditor Entry
Was the Community Programs and Services Audited?		Yes
Has the auditor identified findings, comments, or errors in testing related to community programs and services?		No
If the auditor has identified any ineligible expenditures, please enter the amount here.	0.00	0.00

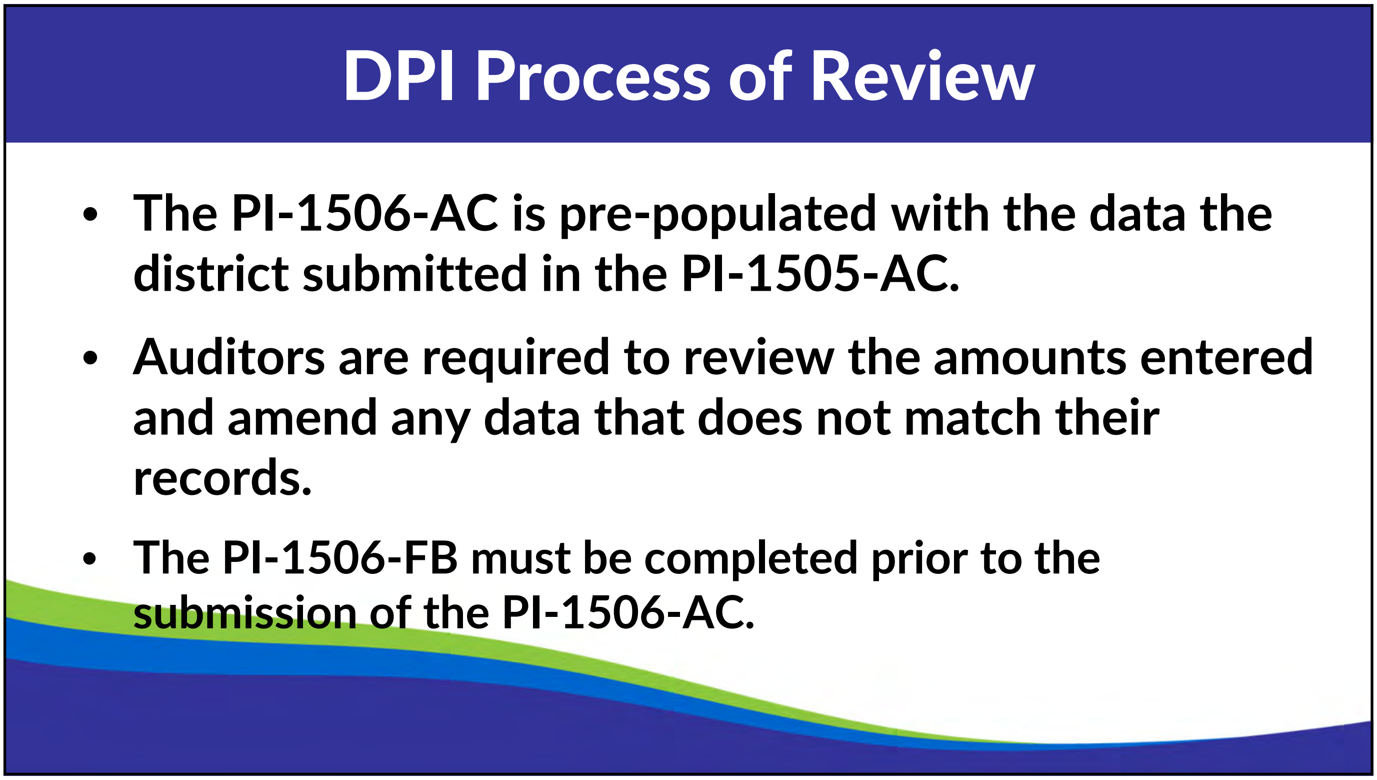
-- If Yes --

You are required to send an email with a description of the findings, comments, or errors in testing including the related amounts.

ANNUAL REPORT & FINANCIAL STATEMENT REVIEW ITEMS

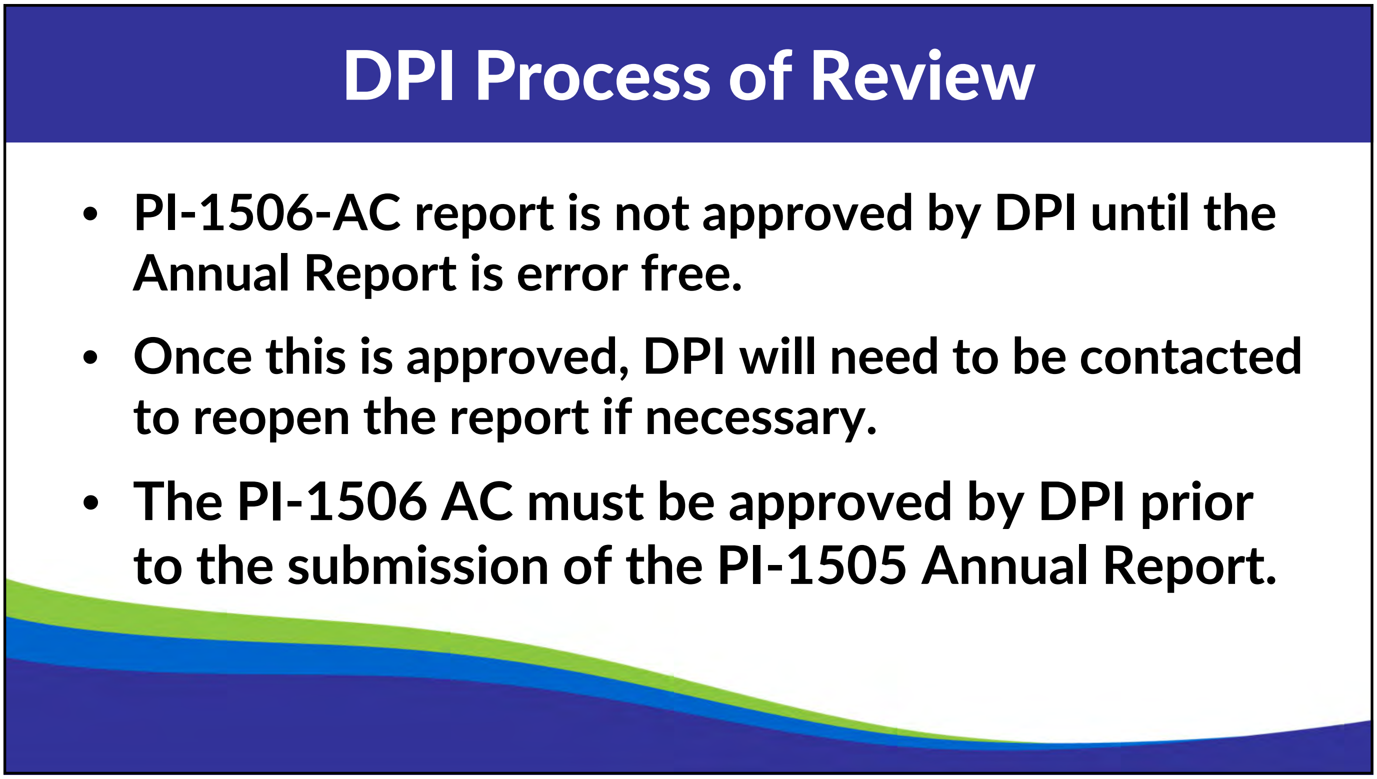
DPI Process of Review

- **The PI-1505-AC is due by the districts.**
- **Approved by DPI, the PI-1506-AC opens**
- **After PI-1505-AC approval, no changes can be made**
  - This may cause variances.



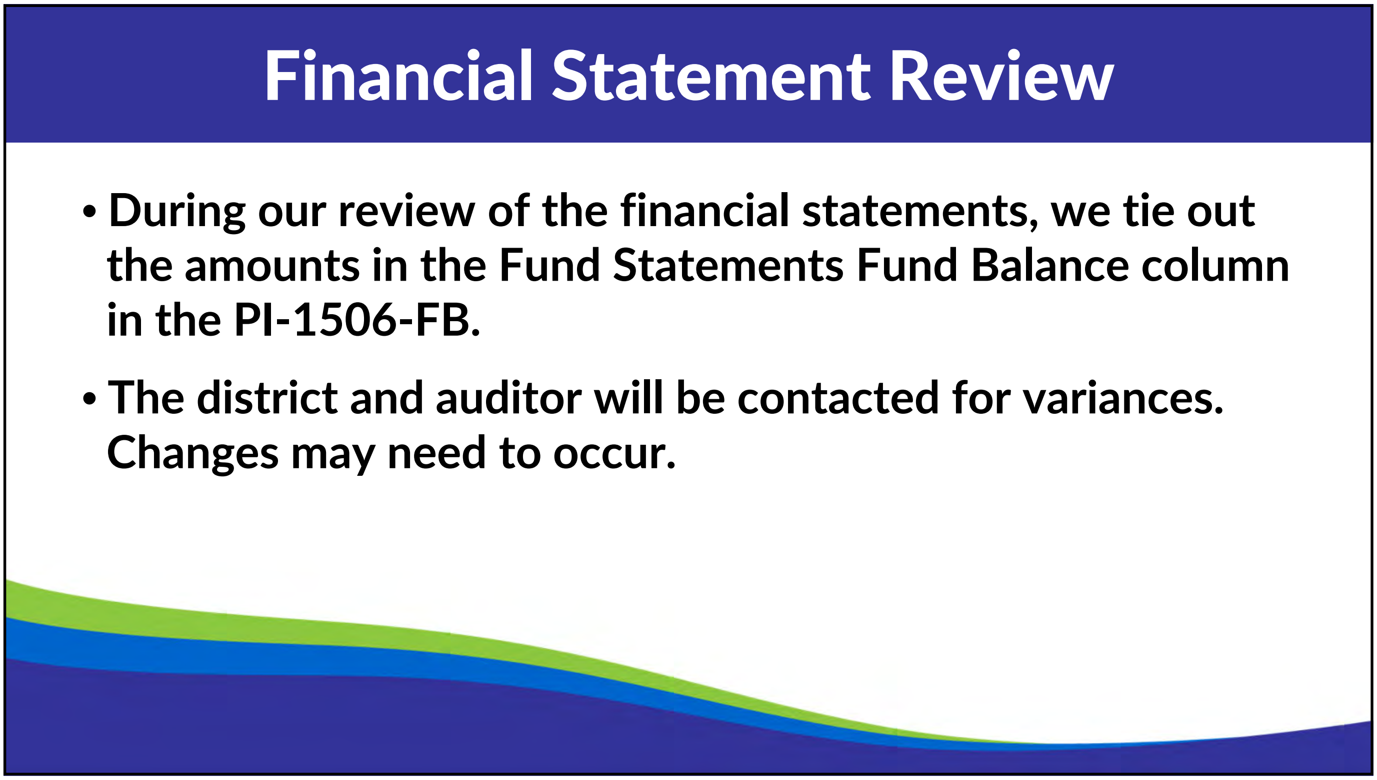
DPI Process of Review

- The PI-1506-AC is pre-populated with the data the district submitted in the PI-1505-AC.
- Auditors are required to review the amounts entered and amend any data that does not match their records.
- The PI-1506-FB must be completed prior to the submission of the PI-1506-AC.



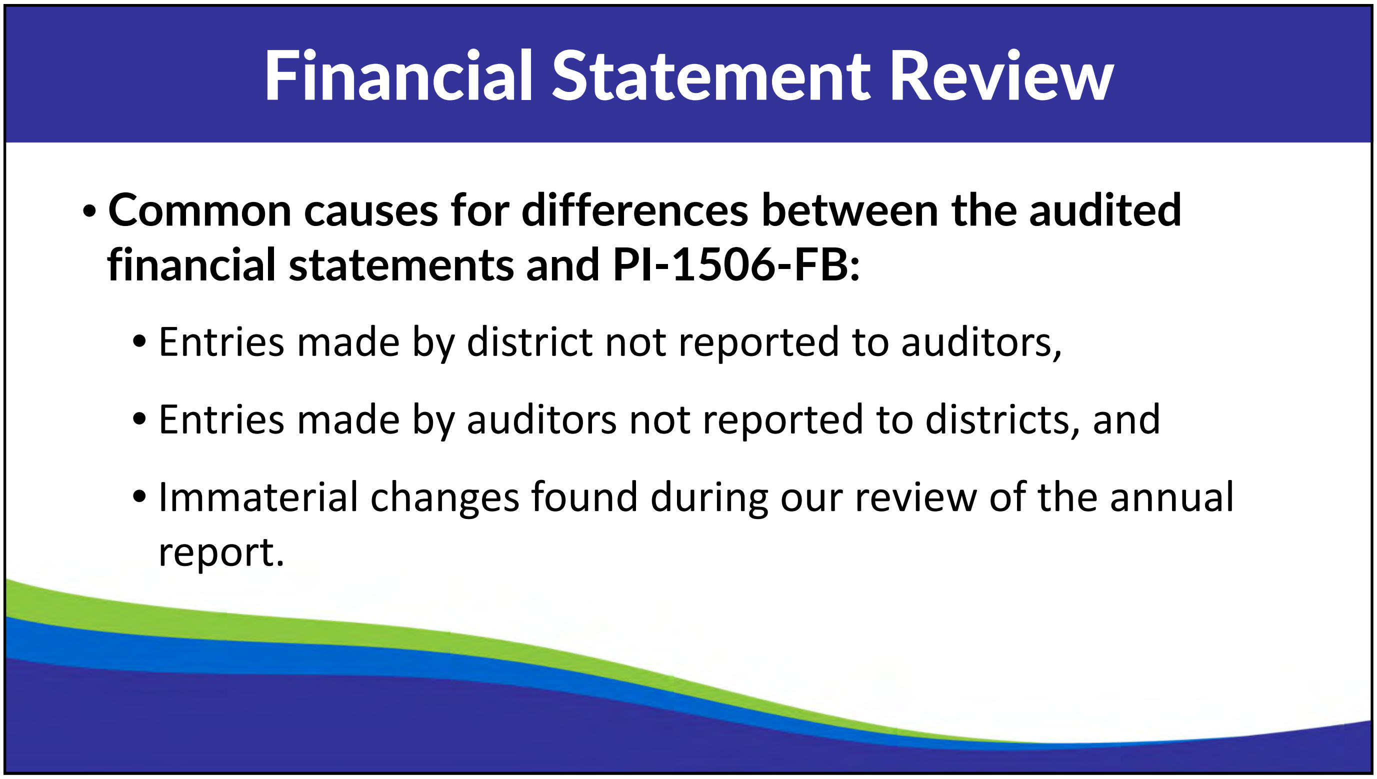
DPI Process of Review

- PI-1506-AC report is not approved by DPI until the Annual Report is error free.
- Once this is approved, DPI will need to be contacted to reopen the report if necessary.
- The PI-1506 AC must be approved by DPI prior to the submission of the PI-1505 Annual Report.



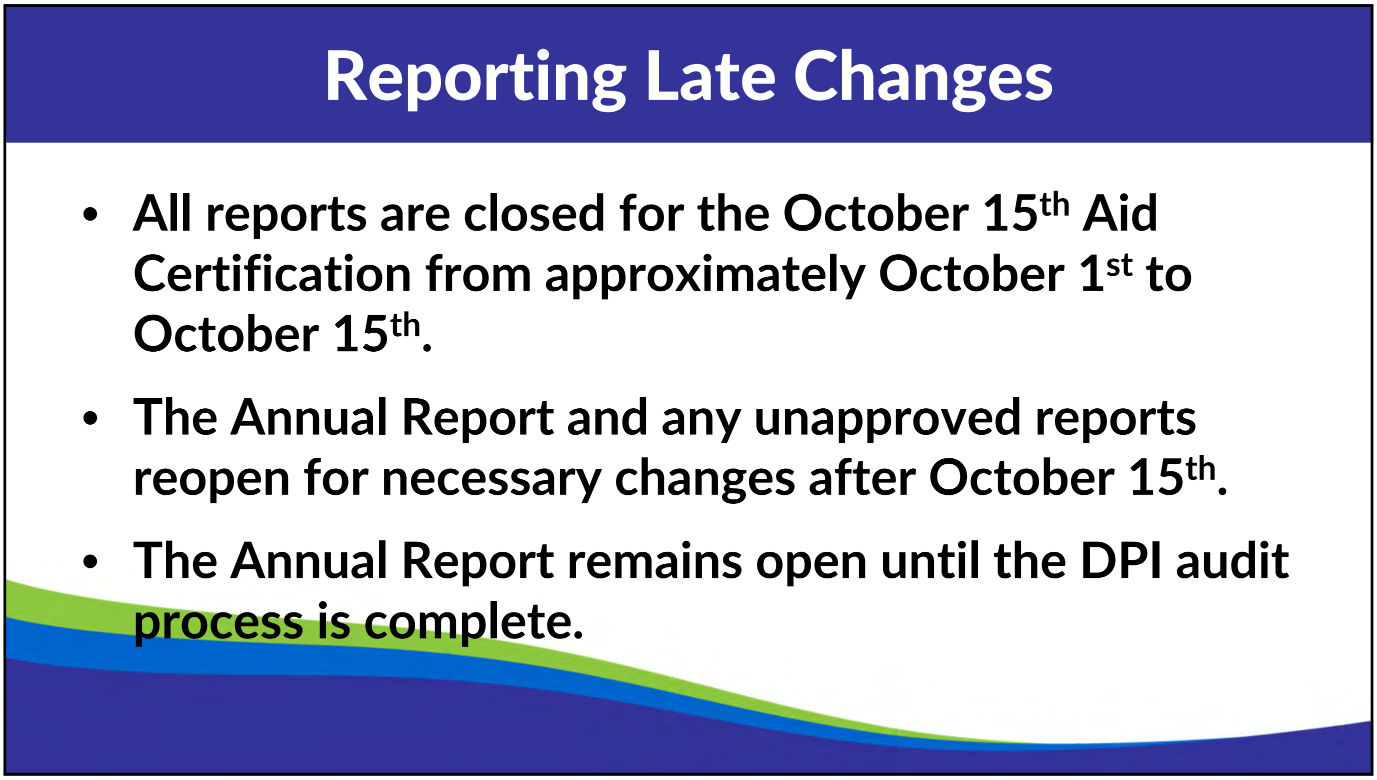
Financial Statement Review

- **During our review of the financial statements, we tie out the amounts in the Fund Statements Fund Balance column in the PI-1506-FB.**
- **The district and auditor will be contacted for variances. Changes may need to occur.**



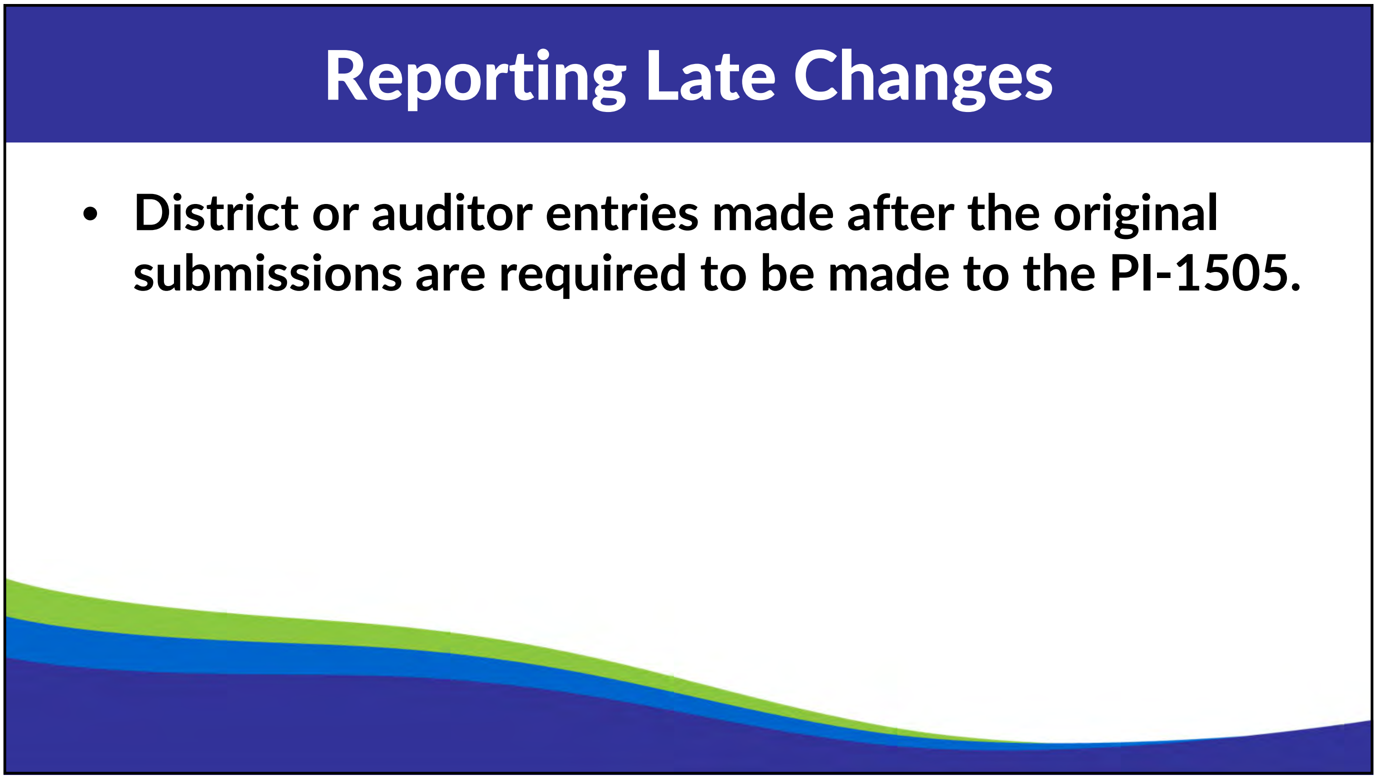
Financial Statement Review

- **Common causes for differences between the audited financial statements and PI-1506-FB:**
  - Entries made by district not reported to auditors,
  - Entries made by auditors not reported to districts, and
  - Immaterial changes found during our review of the annual report.



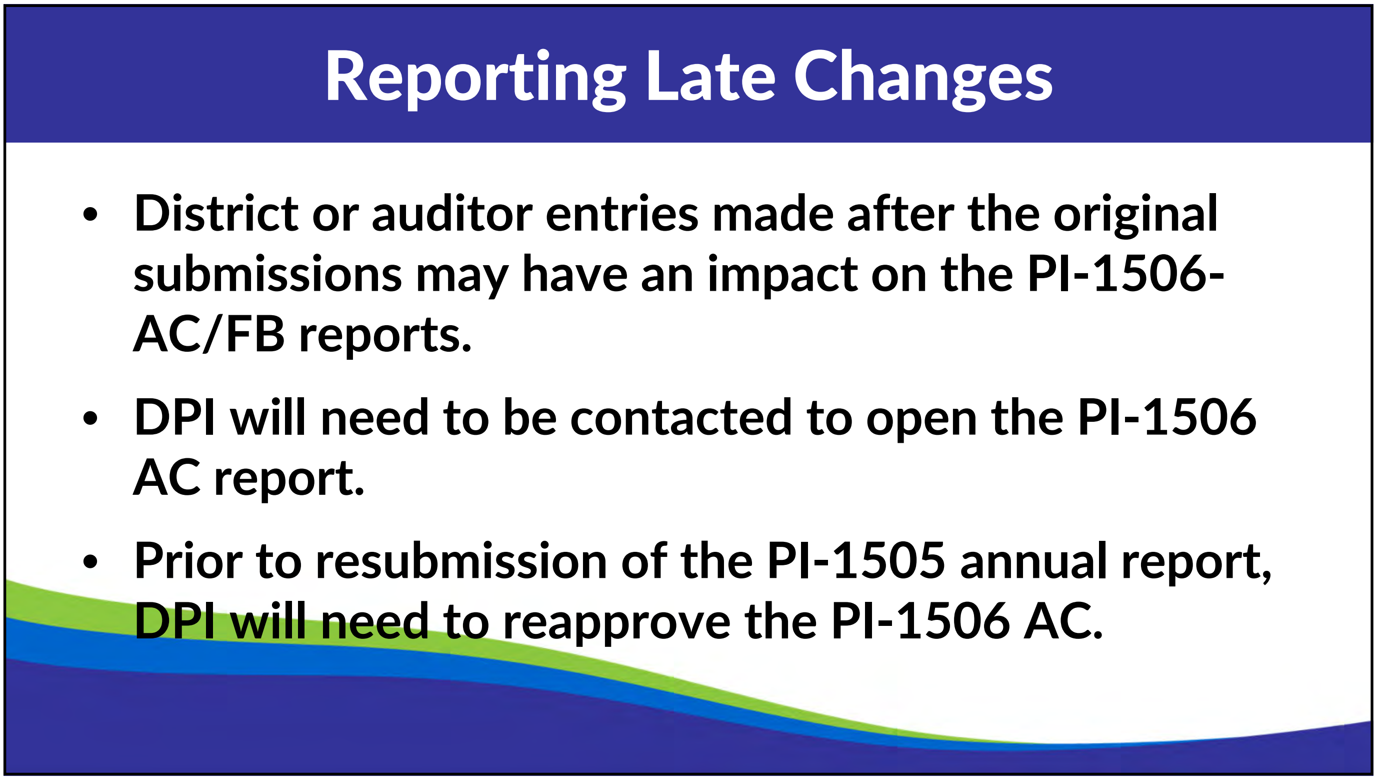
Reporting Late Changes

- All reports are closed for the October 15th Aid Certification from approximately October 1st to October 15th.
- The Annual Report and any unapproved reports reopen for necessary changes after October 15th.
- The Annual Report remains open until the DPI audit process is complete.



Reporting Late Changes

- District or auditor entries made after the original submissions are required to be made to the PI-1505.



Reporting Late Changes

- District or auditor entries made after the original submissions may have an impact on the PI-1506-AC/FB reports.
- DPI will need to be contacted to open the PI-1506 AC report.
- Prior to resubmission of the PI-1505 annual report, DPI will need to reapprove the PI-1506 AC.

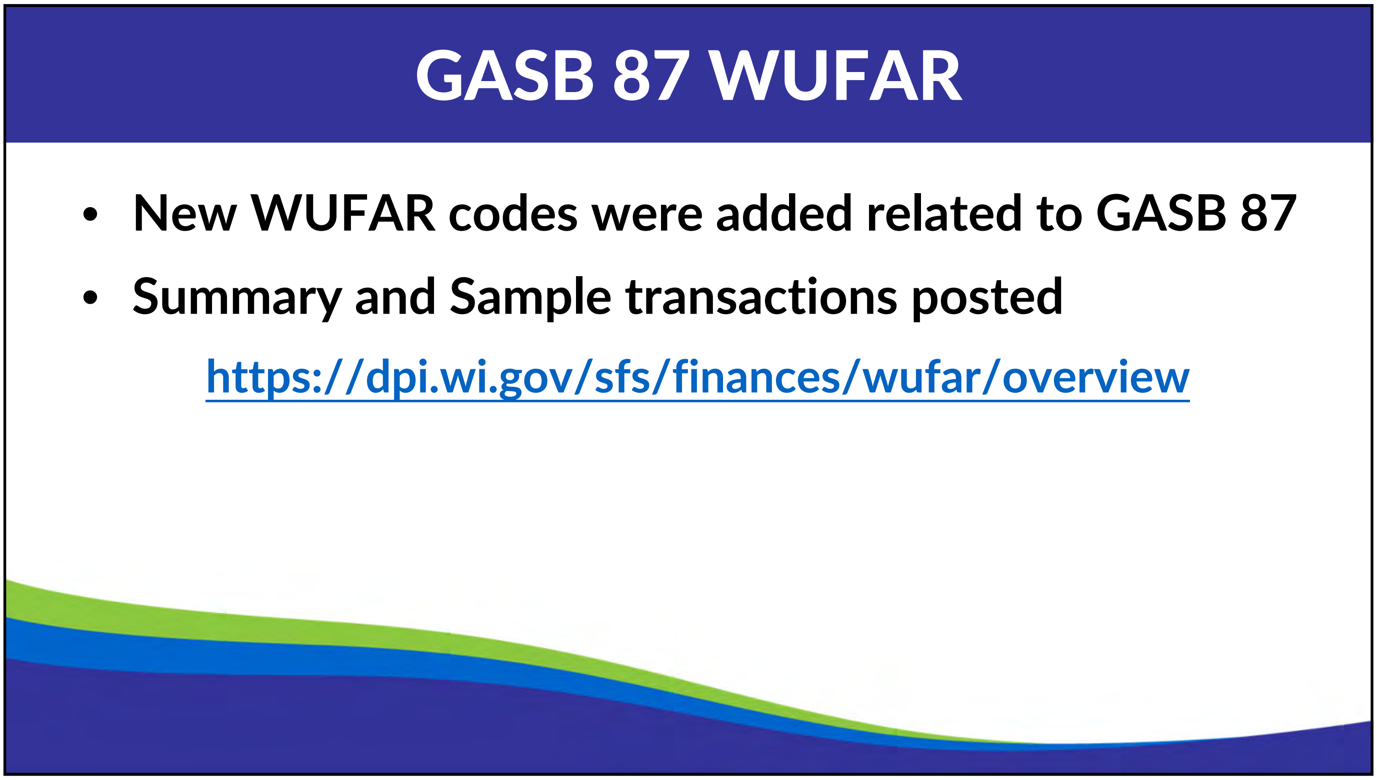
GASB 87
Leases

GASB 87

- Effective for FY22
- Clarifies accounting and financial reporting for leases.
- Must be applied to existing leases as well as new leases.

GASB 87

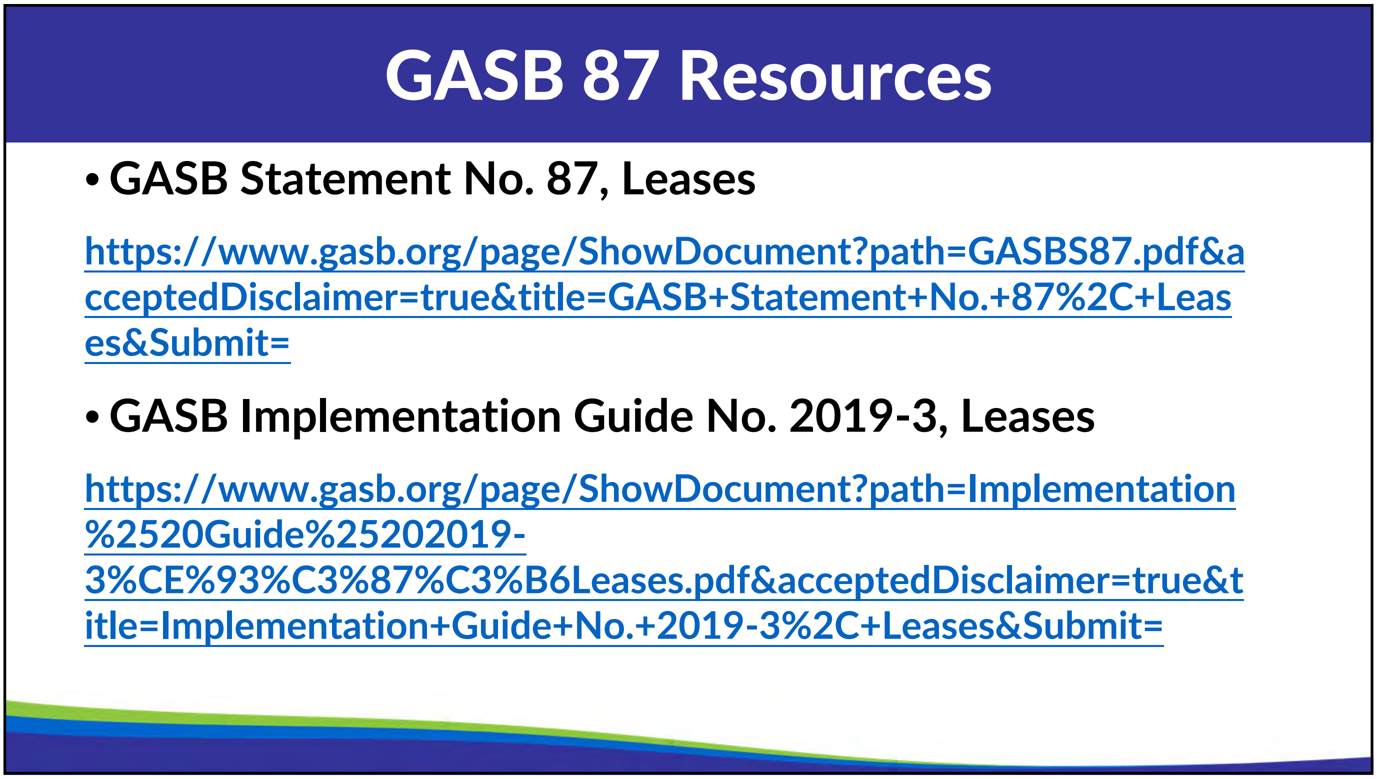
- Districts should be aware of this implementation and should be compiling all contracts.
- Has been communicated by auditors



GASB 87 WUFAR

- New WUFAR codes were added related to GASB 87
- Summary and Sample transactions posted

https://dpi.wi.gov/sfs/finances/wufar/overview



GASB 87 Resources

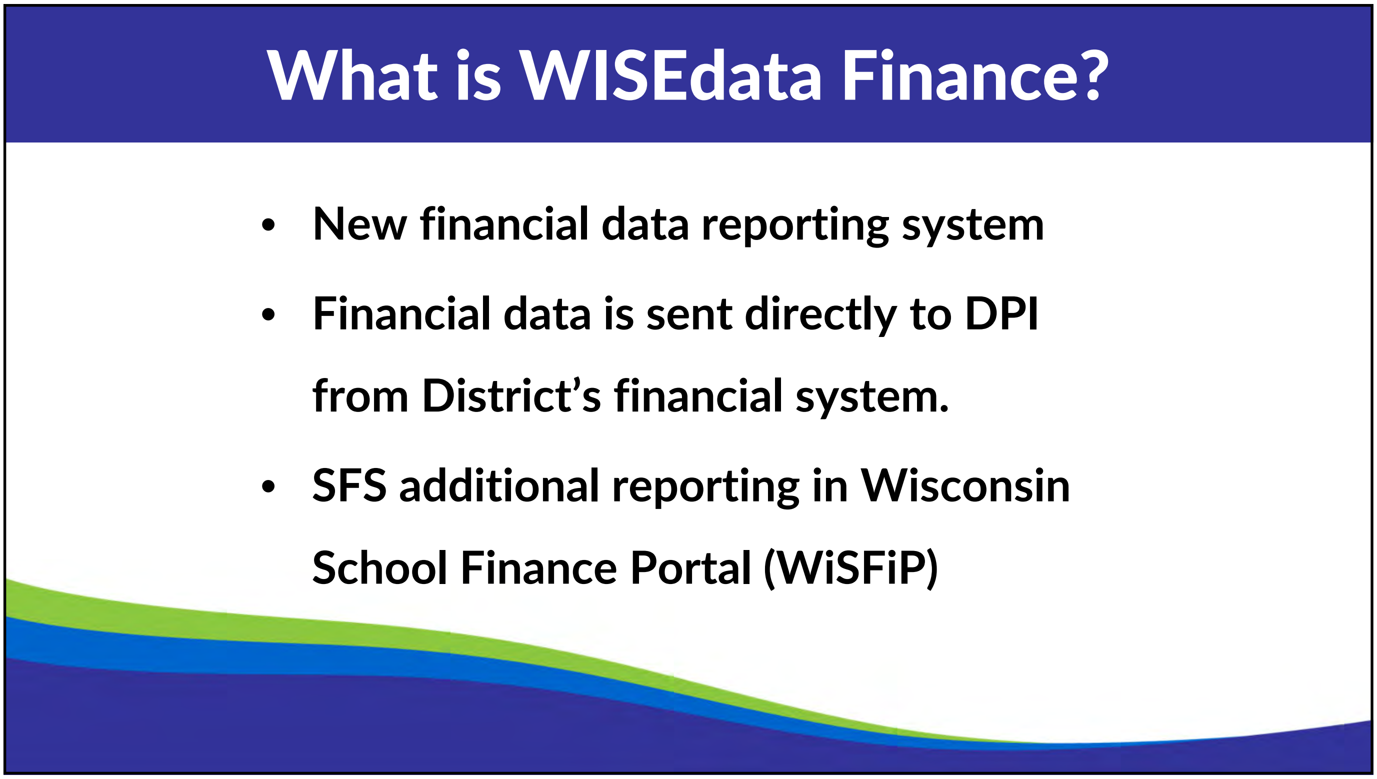
- GASB Statement No. 87, Leases

https://www.gasb.org/page/ShowDocument?path=GASBS87.pdf&acceptedDisclaimer=true&title=GASB+Statement+No.+87%2C+Leases&Submit=

- GASB Implementation Guide No. 2019-3, Leases

https://www.gasb.org/page/ShowDocument?path=Implementation%2520Guide%25202019-3%CE%93%C3%87%C3%B6Leases.pdf&acceptedDisclaimer=true&title=Implementation+Guide+No.+2019-3%2C+Leases&Submit=

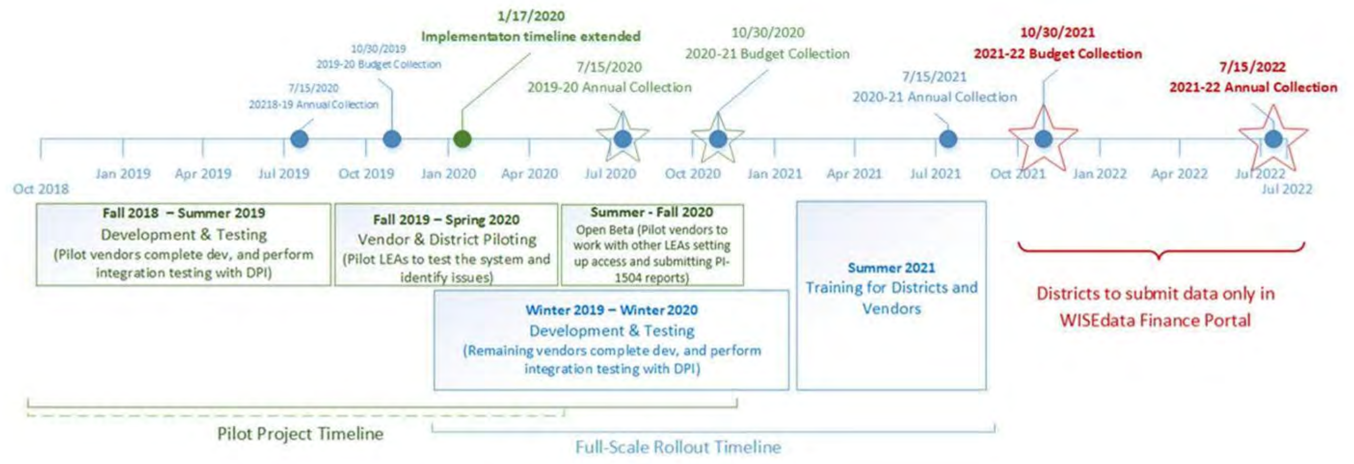
WISEdata Finance/WiSFiP



What is WISEdata Finance?

- New financial data reporting system
- Financial data is sent directly to DPI from District’s financial system.
- SFS additional reporting in Wisconsin School Finance Portal (WiSFiP)

WISEdata Finance Timeline


1/17/2020
Implementaton timeline extended
10/30/2019
2019-20 Budget Collection
7/15/2020
20218-19 Annual Collection
7/15/2020
2019-20 Annual Collection
10/30/2020
2020-21 Budget Collection
7/15/2021
2020-21 Annual Collection
10/30/2021
2021-22 Budget Collection
7/15/2022
2021-22 Annual Collection
Oct 2018
Jan 2019
Apr 2019
Jul 2019
Oct 2019
Jan 2020
Apr 2020
Jul 2020
Oct 2020
Jan 2021
Apr 2021
Jul 2021
Oct 2021
Jan 2022
Apr 2022
Jul 2022
Jul 2022
Pilot Project Timeline
Full-Scale Rollout Timeline

Fall 2018 – Summer 2019
Development & Testing
(Pilot vendors complete dev, and perform integration testing with DPI)

Fall 2019 – Spring 2020
Vendor & District Piloting
(Pilot LEAs to test the system and identify issues)

Summer - Fall 2020
Open Beta (Pilot vendors to work with other LEAs setting up access and submitting PI-1504 reports)

Winter 2019 – Winter 2020
Development & Testing
(Remaining vendors complete dev, and perform integration testing with DPI)

Summer 2021
Training for Districts and Vendors

Districts to submit data only in WISEdata Finance Portal

Current PI-1504/PI-1505 Budget & Annual Reports are still required for 2020-21 reporting.

UPDATED WISEdata Finance Timeline

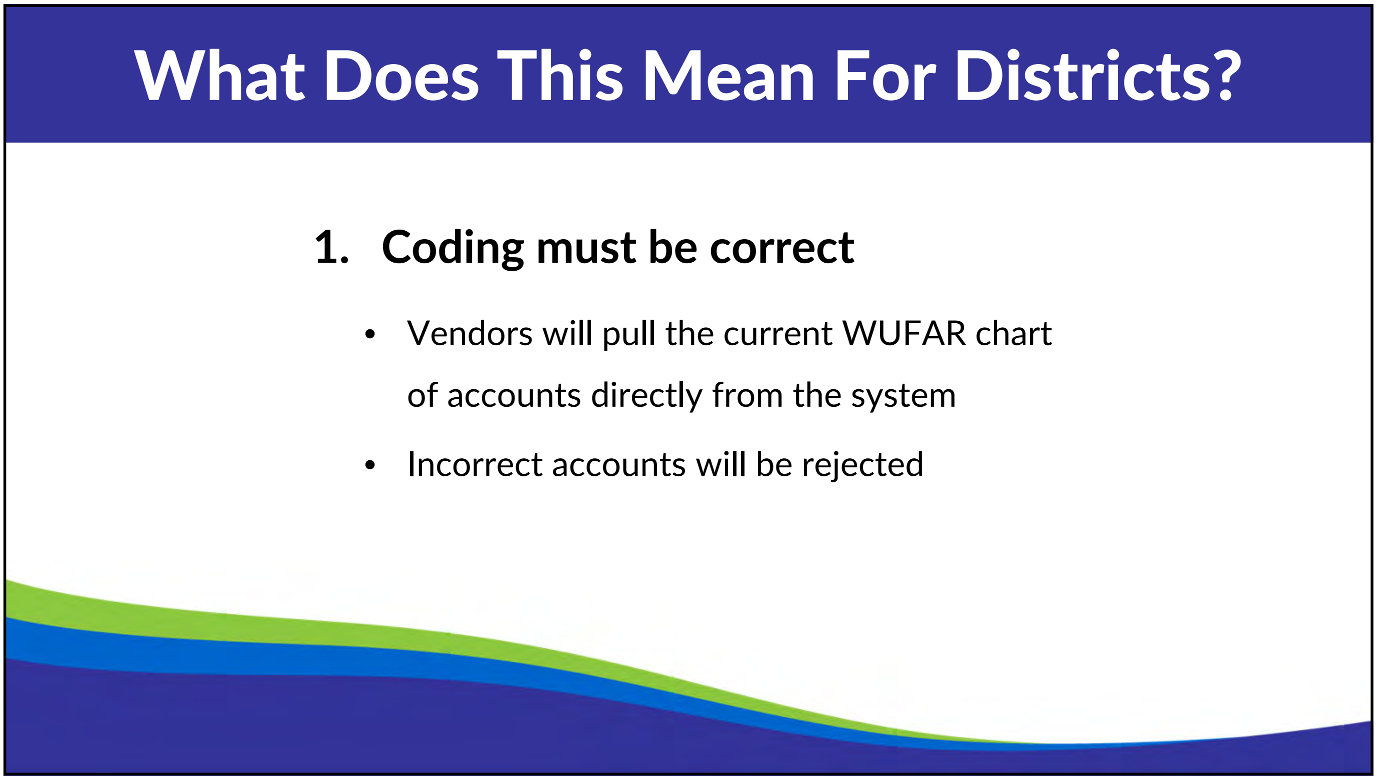
- Districts will be dual reporting for the FY22 Annual Report.
- Budget report was all in WDF, no PI-1504 for FY22

Why WISEdata Finance?

- Eliminate the manual part of financial reporting
- Better consistency with DPI and local accounts side by side
- Easier reporting compliance (CRDC, ESSA School Level, PI-1504/1505, etc.)

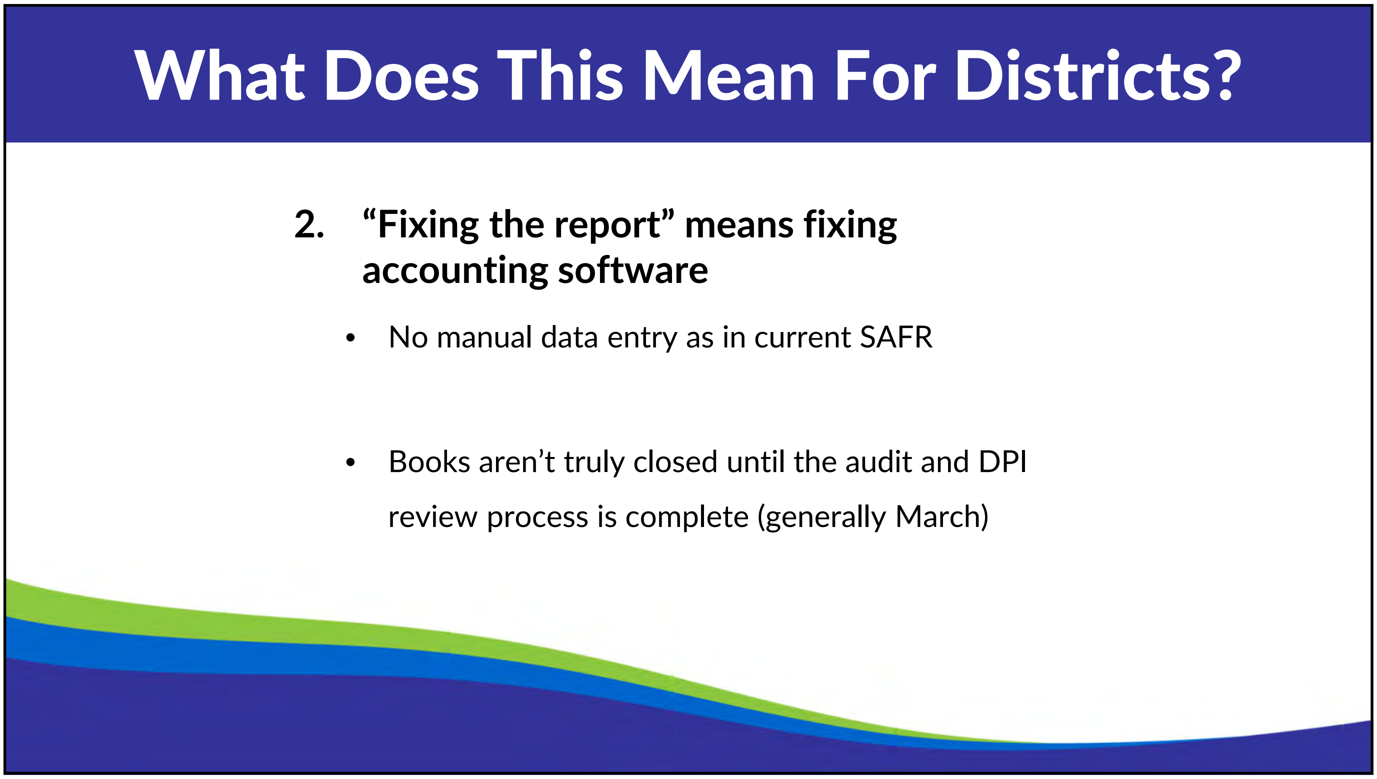
How Does WISEdata Finance Work?

1. Vendors pull the current WUFAR Chart of Accounts from DPI
2. District pushes a crosswalk between local COA and WUFAR to DPI
3. District pushes budgets & YTD actuals by account to DPI



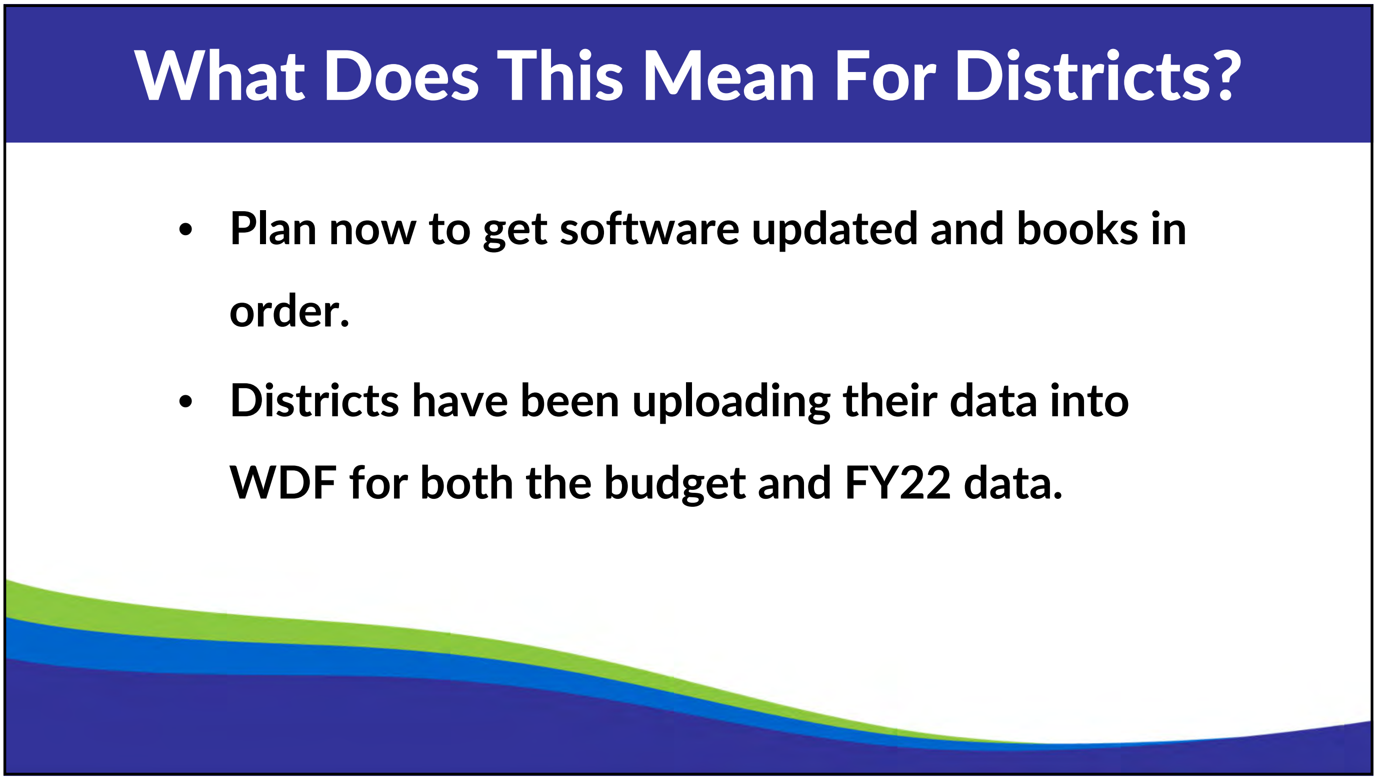
What Does This Mean For Districts?

1. **Coding must be correct**
   - Vendors will pull the current WUFAR chart of accounts directly from the system
   - Incorrect accounts will be rejected



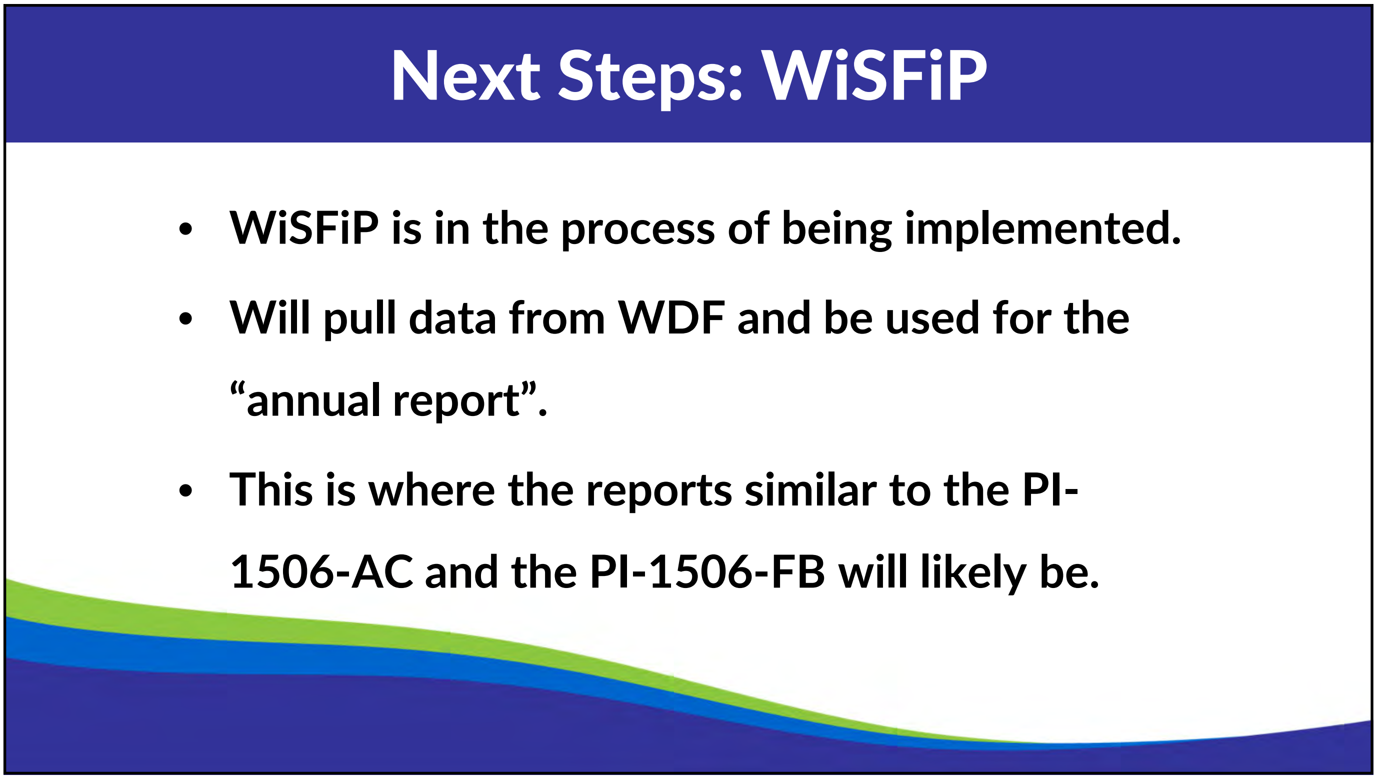
What Does This Mean For Districts?

2. **“Fixing the report” means fixing accounting software**
   - No manual data entry as in current SAFR
   - Books aren’t truly closed until the audit and DPI review process is complete (generally March)



What Does This Mean For Districts?

- Plan now to get software updated and books in order.
- Districts have been uploading their data into WDF for both the budget and FY22 data.



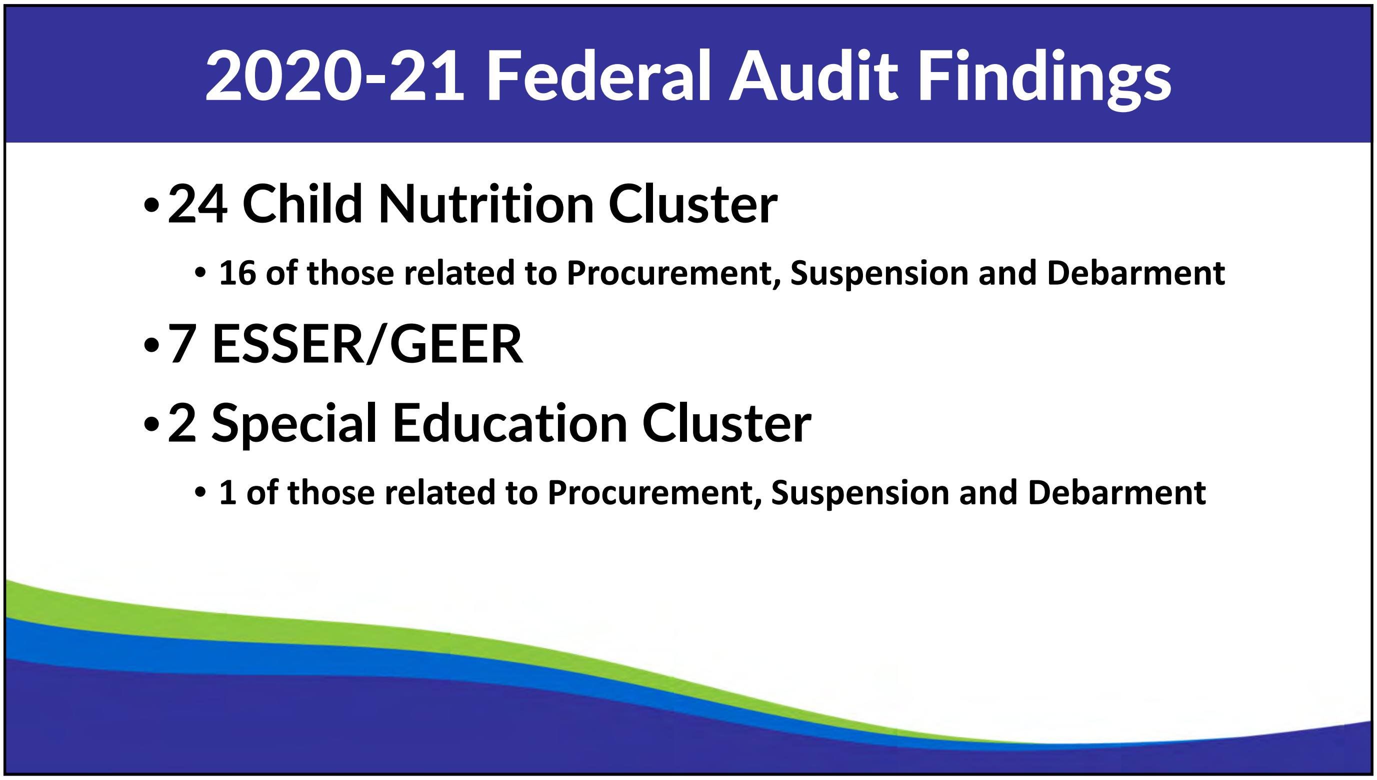
Next Steps: WiSFiP

- WiSFiP is in the process of being implemented.
- Will pull data from WDF and be used for the “annual report”.
- This is where the reports similar to the PI-1506-AC and the PI-1506-FB will likely be.

Next Steps: WiSFiP

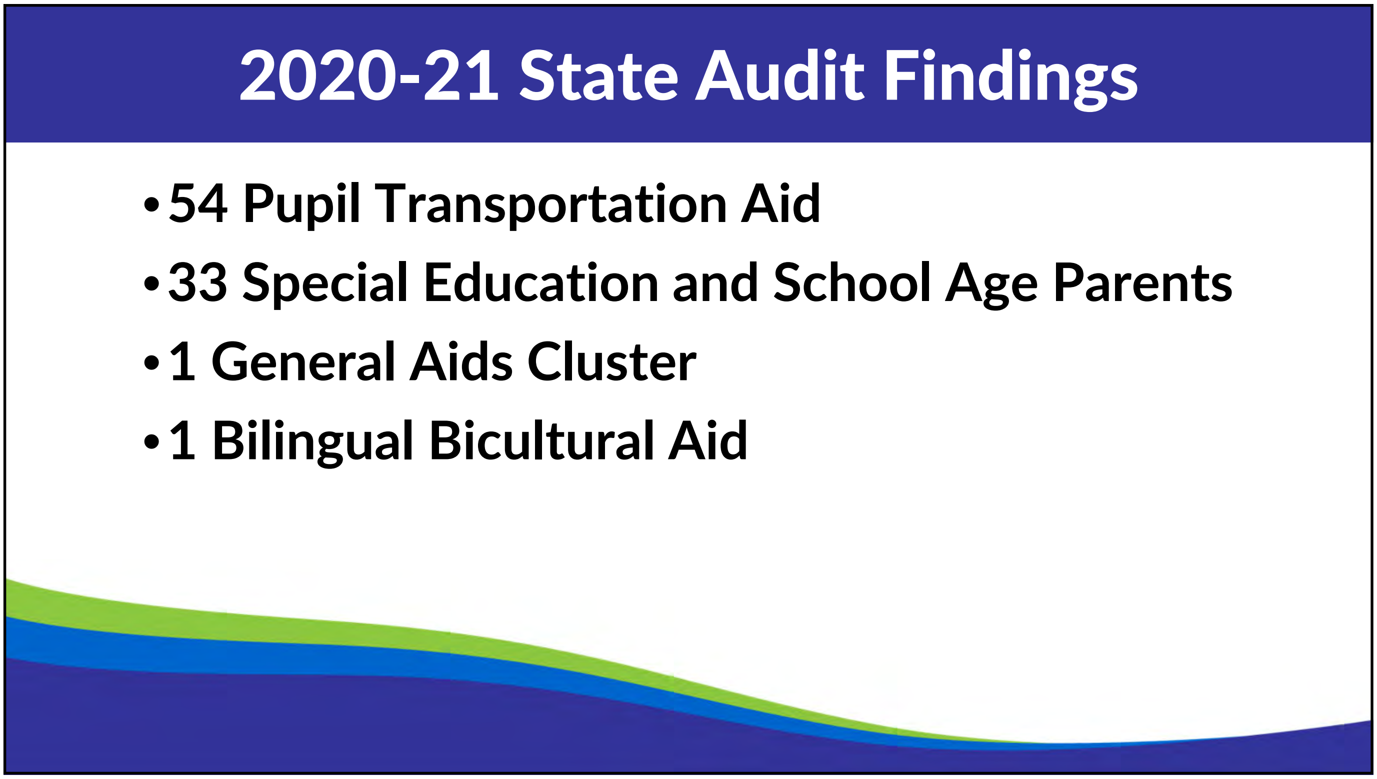
- Auditor reports have yet to be developed.
- Any feedback on the current reports or what you would like to see?

COMMON AUDIT FINDINGS



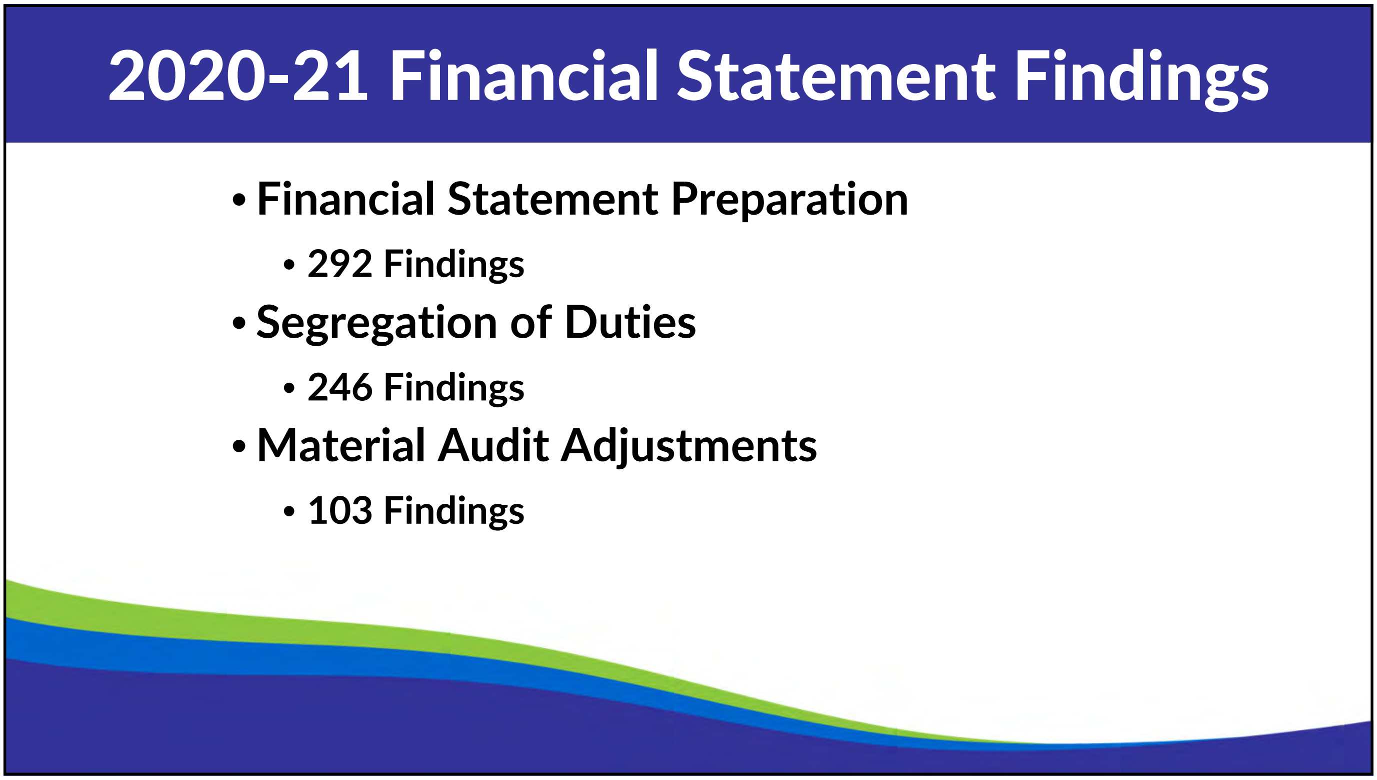
2020-21 Federal Audit Findings

- 24 Child Nutrition Cluster
  - 16 of those related to Procurement, Suspension and Debarment
- 7 ESSER/GEER
- 2 Special Education Cluster
  - 1 of those related to Procurement, Suspension and Debarment



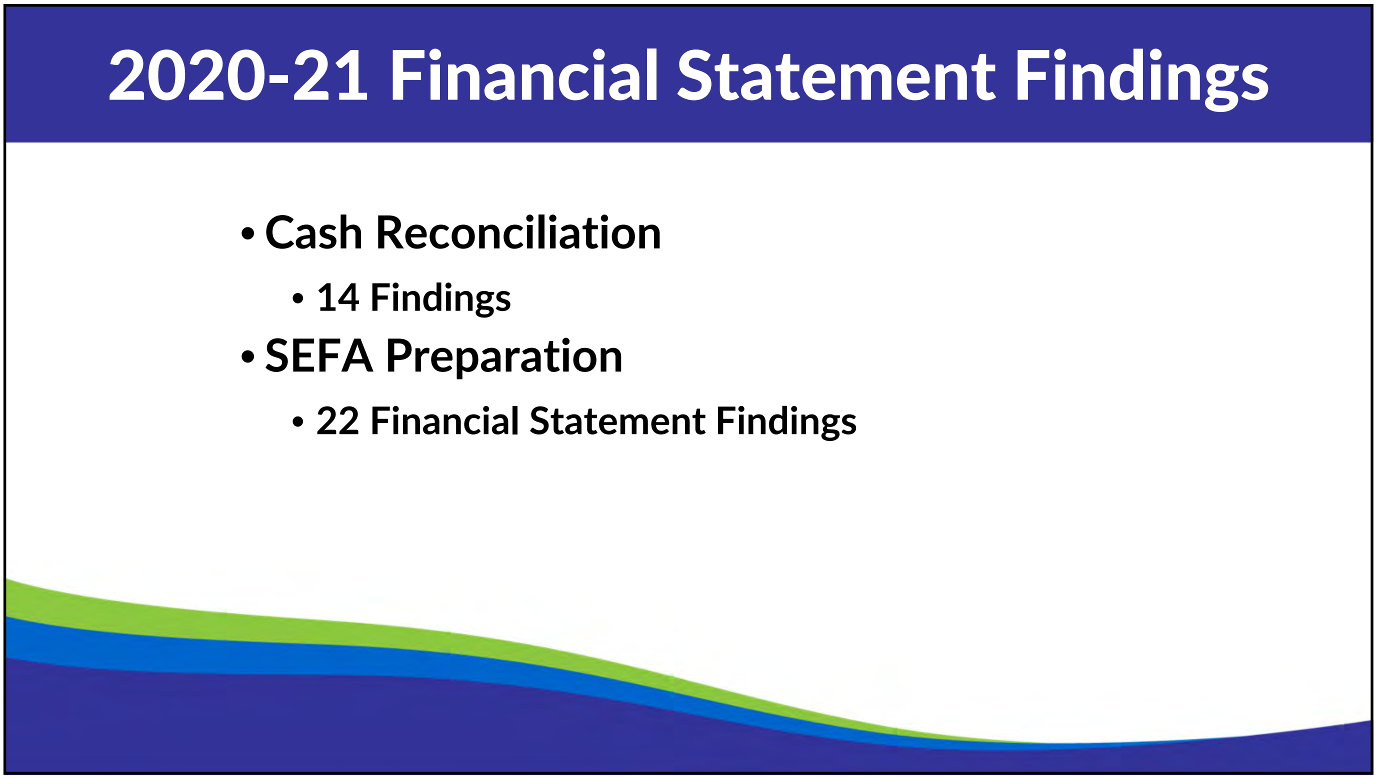
2020-21 State Audit Findings

- 54 Pupil Transportation Aid
- 33 Special Education and School Age Parents
- 1 General Aids Cluster
- 1 Bilingual Bicultural Aid



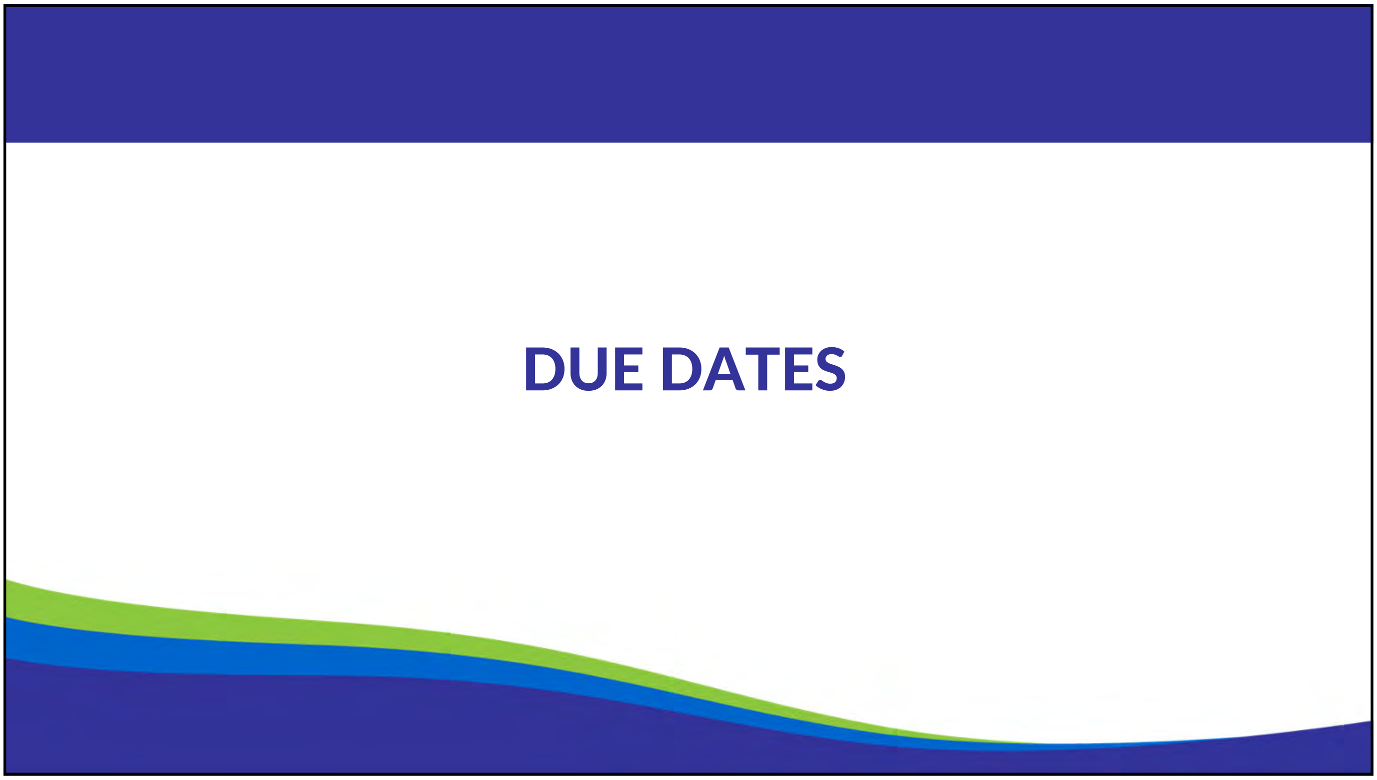
2020-21 Financial Statement Findings

- Financial Statement Preparation
  - 292 Findings
- Segregation of Duties
  - 246 Findings
- Material Audit Adjustments
  - 103 Findings

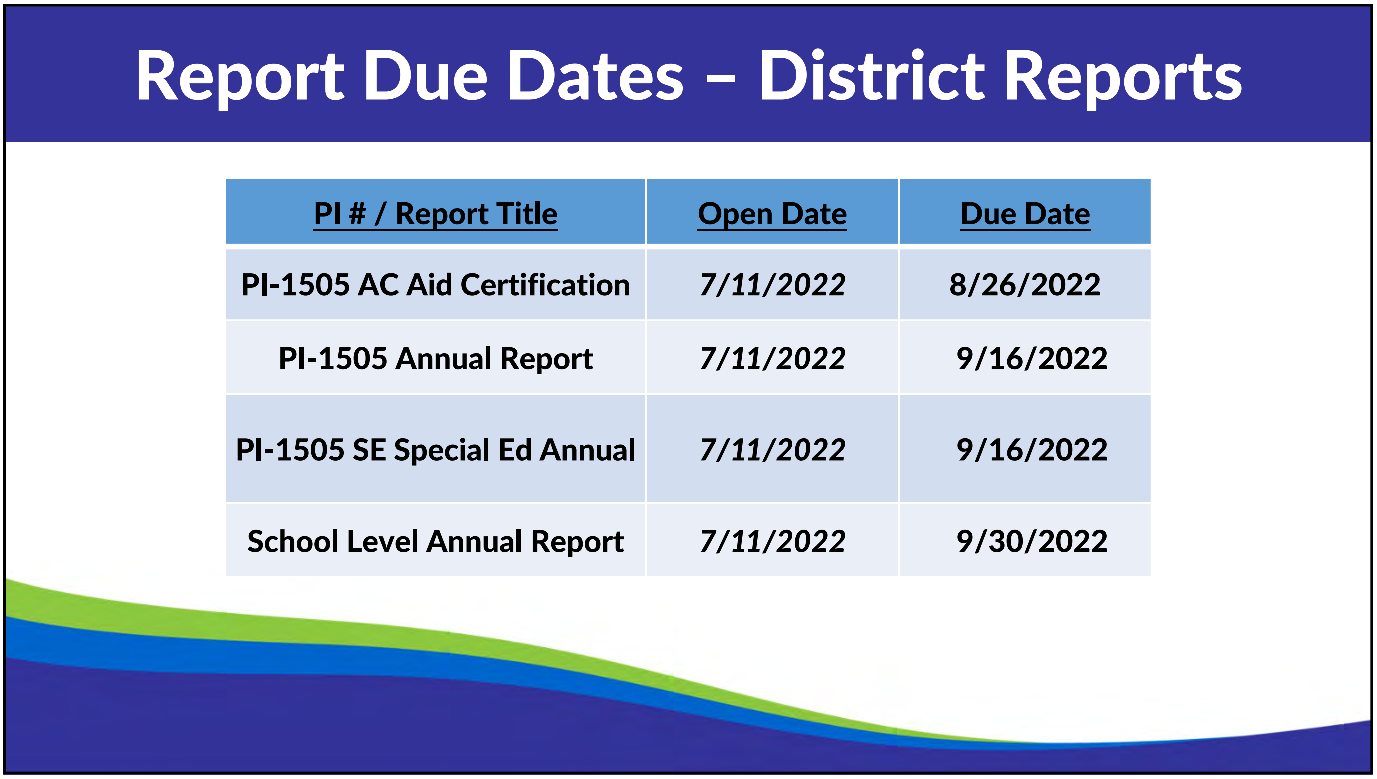


2020-21 Financial Statement Findings

- Cash Reconciliation
  - 14 Findings
- SEFA Preparation
  - 22 Financial Statement Findings

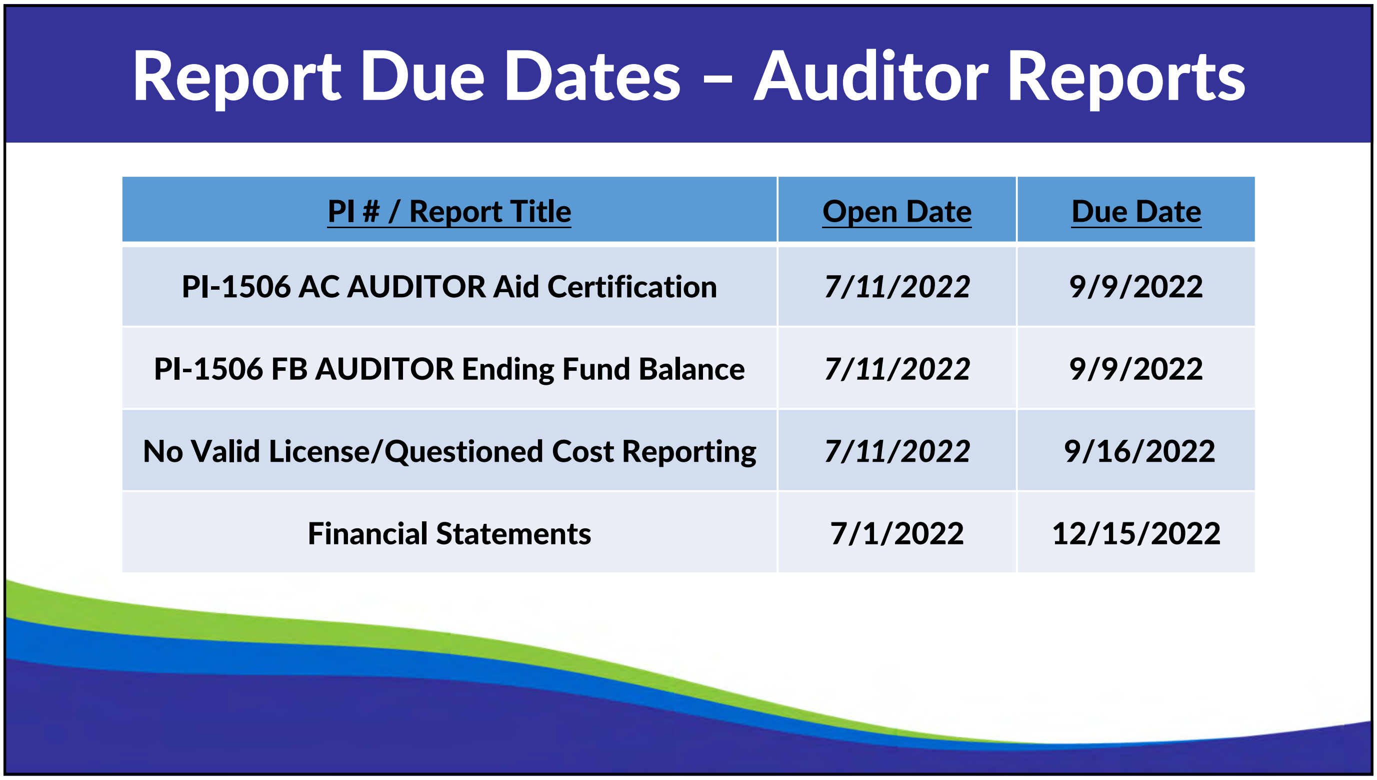


DUE DATES



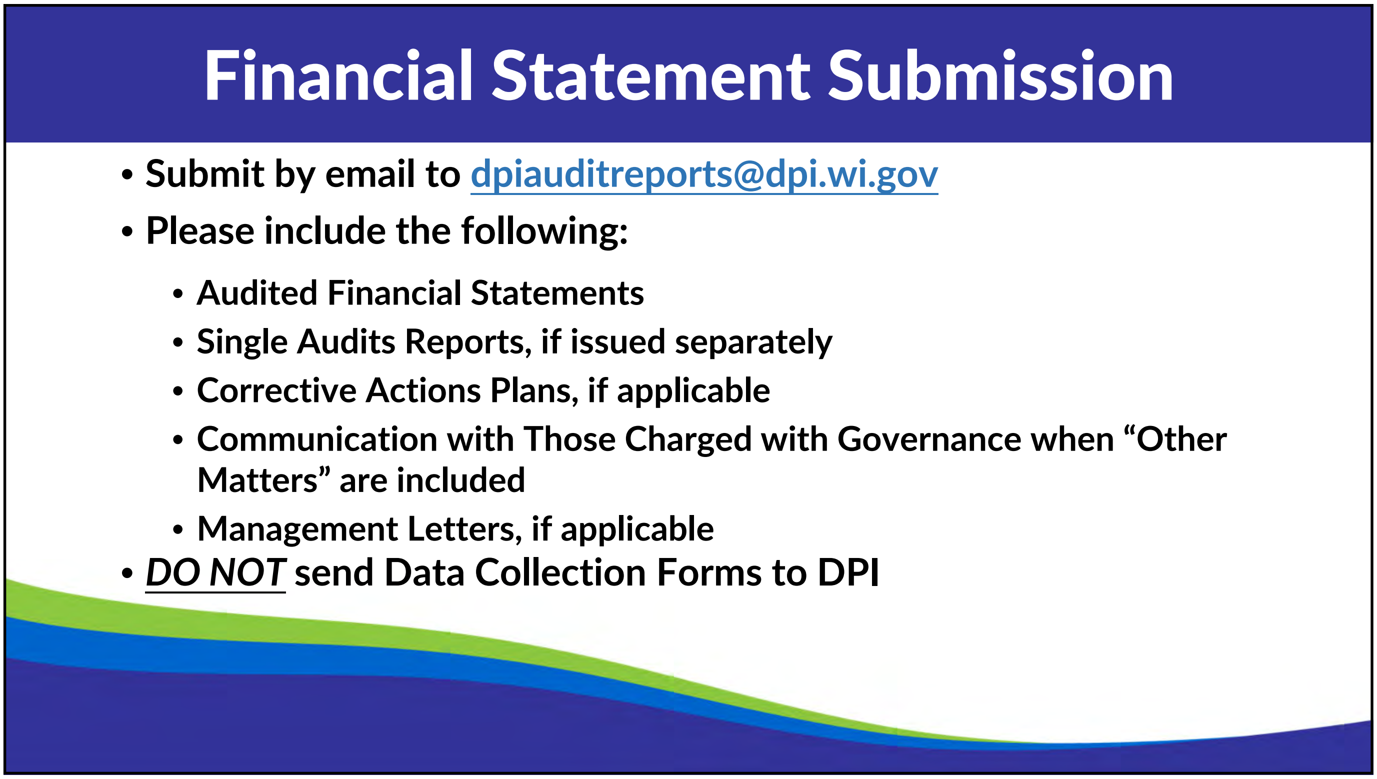
Report Due Dates – District Reports

PI # / Report Title	Open Date	Due Date
PI-1505 AC Aid Certification	7/11/2022	8/26/2022
PI-1505 Annual Report	7/11/2022	9/16/2022
PI-1505 SE Special Ed Annual	7/11/2022	9/16/2022
School Level Annual Report	7/11/2022	9/30/2022



Report Due Dates – Auditor Reports

PI # / Report Title	Open Date	Due Date
PI-1506 AC AUDITOR Aid Certification	*7/11/2022*	9/9/2022
PI-1506 FB AUDITOR Ending Fund Balance	*7/11/2022*	9/9/2022
No Valid License/Questioned Cost Reporting	*7/11/2022*	9/16/2022
Financial Statements	7/1/2022	12/15/2022

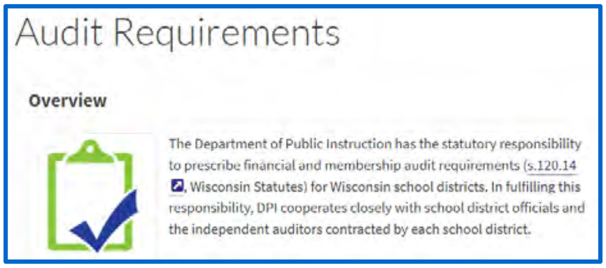


Financial Statement Submission

- Submit by email to dpiauditreports@dpi.wi.gov
- Please include the following:
  - Audited Financial Statements
  - Single Audits Reports, if issued separately
  - Corrective Actions Plans, if applicable
  - Communication with Those Charged with Governance when “Other Matters” are included
  - Management Letters, if applicable
- *DO NOT* send Data Collection Forms to DPI

Timely Reporting to DPI Impacts Us All

- Late submission of SAFR reports
- Late submission of audited financial statements
- Late submission of Actuarial studies



Audit Requirements

Overview

The Department of Public Instruction has the statutory responsibility to prescribe financial and membership audit requirements (s.120.14, Wisconsin Statutes) for Wisconsin school districts. In fulfilling this responsibility, DPI cooperates closely with school district officials and the independent auditors contracted by each school district.

Peer Review Letters

- Peer review letters
  - SFS team reviews firm peer review letters
  - Please send any updated peer review letters as soon as available
  - DPIauditreports@dpi.wi.gov

Questions? Comments?

Subscribe to Auditor Listserv

Contact Information

Olivia Bernitt
SFS Auditor
olivia.bernitt@dpi.wi.gov
608-261-2137

General Contact Information
https://dpi.wi.gov/sfs
DPIfin@dpi.wi.gov
608-267-9114

9:50 – 11:30 a.m.

Cybersecurity Threats, Trends & Strategies

Mark Scholl, MCSE, CISA, CISSP CEH, *Principal, Wipfli LLP*

Cybersecurity Hot Topics

The Latest Trends

May 24, 2022

wipfli.com

WIPFLI

Contact information

Mark Scholl
Principal
Wipfli LLP
815.626.1277
mscholl@wipfli.com

Certified Ethical Hacker (CEH)

Certified Information Systems Auditor (CISA)

Certified Information Systems Security Professional (CISSP)

Microsoft Certified Systems Engineer (MCSE)

Agenda:

- Cybersecurity Trends
- Case Study
- Risk Management
- Resources

Cybersecurity Trends

Cybersecurity threats and trends – Threat actors

2021 Verizon Cyber Espionage Report

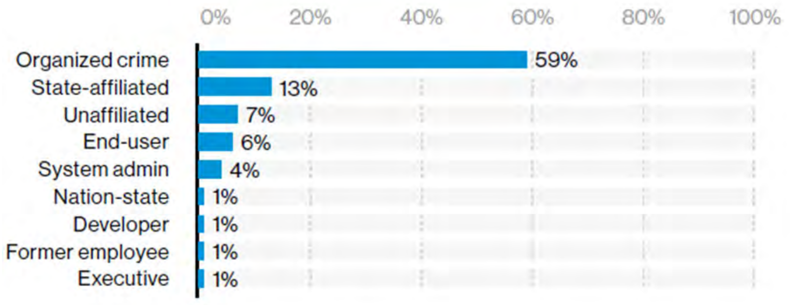
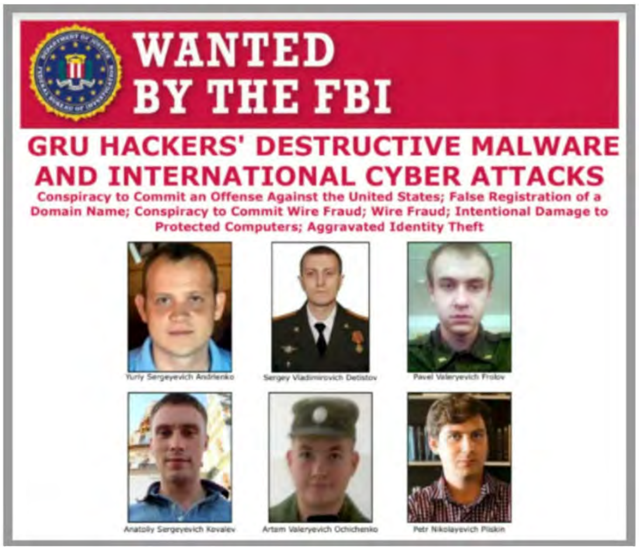


Figure #35: Actor varieties within all breaches (2014-2020 DBIR; n=9,077)

Cybersecurity threats and trends – State sponsored


WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko
Sergey Vladimirovich Detistov
Pavel Valeryevich Frolov
Anatoliy Sergeyevich Kovalev
Artem Valeryevich Ochichenko
Petr Nikolayevich Pliskin

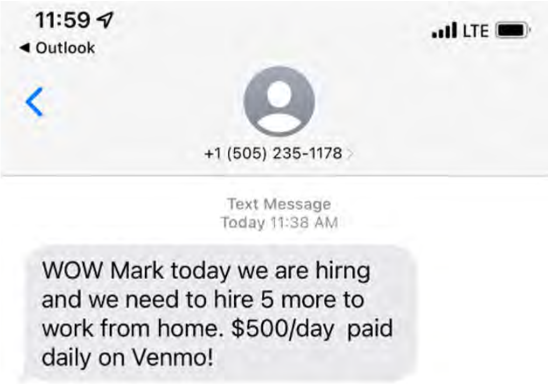
Challenges for law enforcement

- Anonymity
  - Originating IP address is difficult to track
  - Dark web users do not use nicknames, usernames, or email addresses from surface web
- Jurisdictional
  - Extradition rights
  - Digital crime continues to evolve
- Money trail
  - Cryptocurrencies

Phishing types

- SMS phishing (smishing)
  - Phishing attack conducted using SMS (text message) on mobile devices
- Vishing
  - Conducted by phone or voice messages – voice phishing
  - Robo calls
  - Increase in fraudulent calls to call centers
- Email phishing
  - Act of sending emails where an attacker masquerades as a reputable entity

SMS phishing (smishing) example

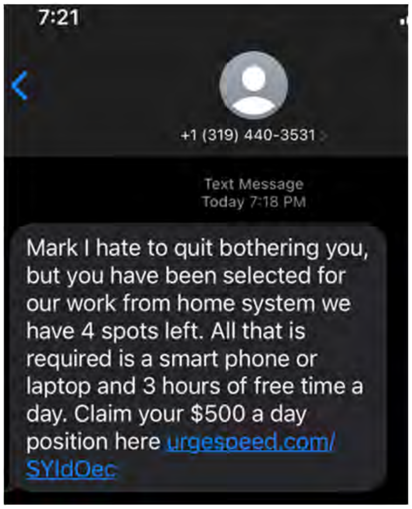


11:59
◀ Outlook
LTE

+1 (505) 235-1178 >

Text Message
Today 11:38 AM

WOW Mark today we are hirng and we need to hire 5 more to work from home. $500/day paid daily on Venmo!



7:21

+1 (319) 440-3531 >

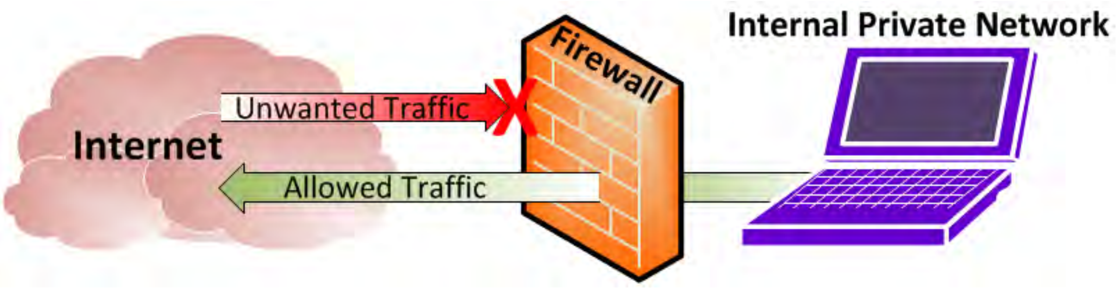
Text Message
Today 7:18 PM

Mark I hate to quit bothering you, but you have been selected for our work from home system we have 4 spots left. All that is required is a smart phone or laptop and 3 hours of free time a day. Claim your $500 a day position here urgespeed.com/SYIdOec

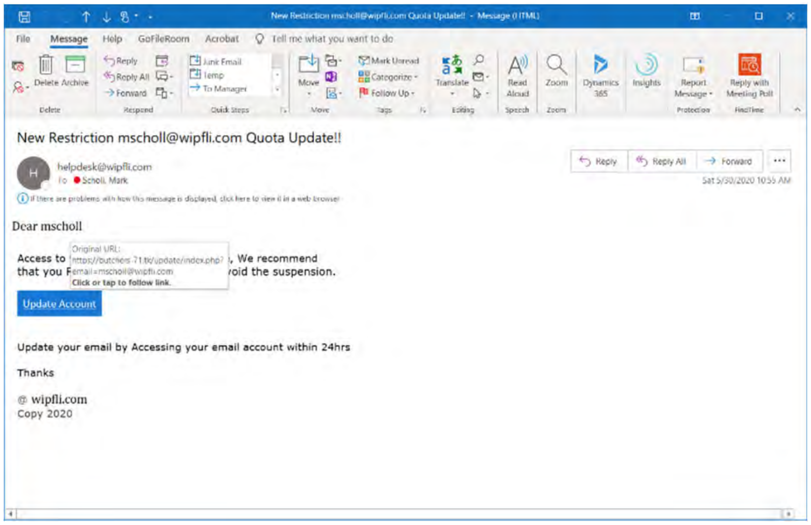
Cybersecurity threats and trends – Email scam types

- Email scams are the attack vector!!!
  - Deliver malicious software
    - Ransomware
    - Backdoors
    - Keyloggers
  - Account takeover
  - Business email compromise (BEC)
  - Extortion

Client-side vulnerability – Email scams



Email phishing example – Password stealing



New Restriction mscholl@wipfli.com Quota Update!!

helpdesk@wipfli.com
To ● Scholl, Mark

Sat 5/30/2020 10:55 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Dear mscholl

Access to , We recommend
that you F oid the suspension.

Original URL:
https://butchers-71.tk/update/index.php?email=mscholl@wipfli.com
Click or tap to follow link.

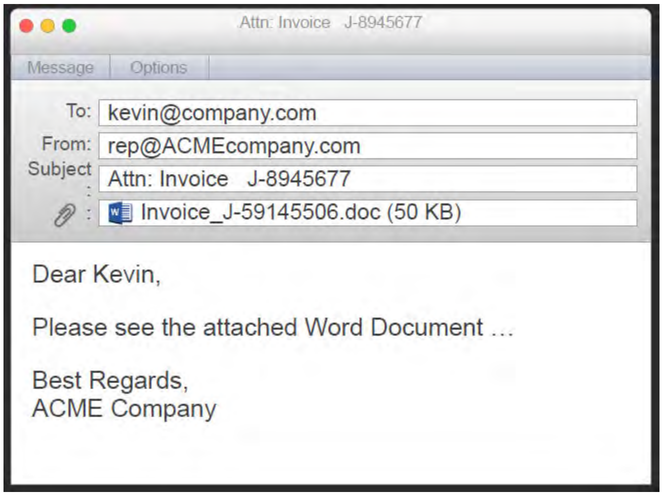
Update Account

Update your email by Accessing your email account within 24hrs

Thanks

@ wipfli.com
Copy 2020

Cyber Threat Trends – Macro Malware



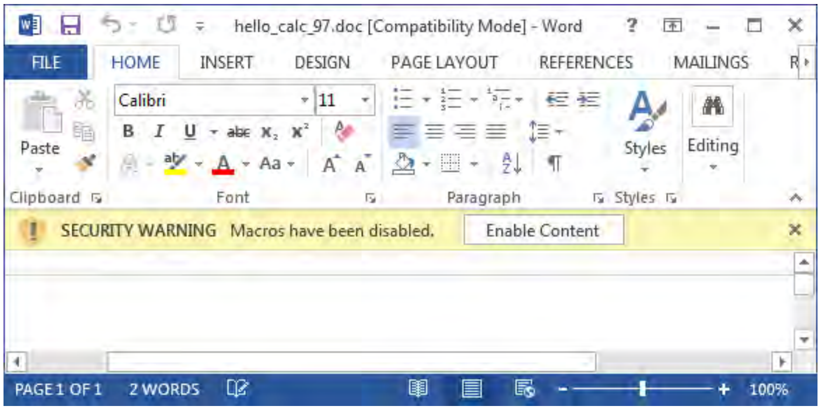
To: kevin@company.com
From: rep@ACMEcompany.com
Subject: Attn: Invoice J-8945677
: Invoice_J-59145506.doc (50 KB)

Dear Kevin,

Please see the attached Word Document …

Best Regards,
ACME Company

Cyber Threat Trends – Macro Malware


hello_calc_97.doc [Compatibility Mode] - Word

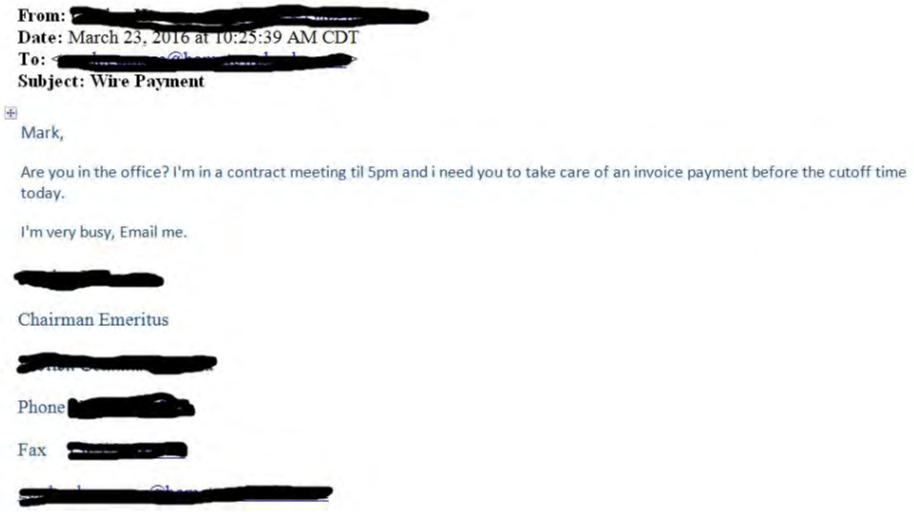
SECURITY WARNING Macros have been disabled. Enable Content

PAGE 1 OF 1 2 WORDS 100%

Cybersecurity trends – Business email compromise (BEC)

- Attacker targets CxO or business owner; attacker gains access to victim's email account or uses a "look-alike" domain to send a message tricking an employee into performing a wire transfer or other identity scam
  - Fraudulent wire transfer
  - Payroll diversion
  - Gift card scam
  - Tech support scam
  - W-2 scams

Business email compromise



From: [redacted]
Date: March 23, 2016 at 10:25:39 AM CDT
To: [redacted]
Subject: Wire Payment

Mark,

Are you in the office? I'm in a contract meeting til 5pm and i need you to take care of an invoice payment before the cutoff time today.

I'm very busy, Email me.

[redacted]

Chairman Emeritus

[redacted]

Phone [redacted]

Fax [redacted]

[redacted]

Supply chain attacks

- Emerging threat that targets software developers and suppliers
- Outside partner or provider with access to your system is infiltrated
  - ▶ Process of infecting legitimate applications
    - Accessing and modifying source code
    - Typically installed through application updates
  - ▶ Examples
    - SolarWinds attack
    - Kaseya
    - Log4j
      - Open-source software libraries

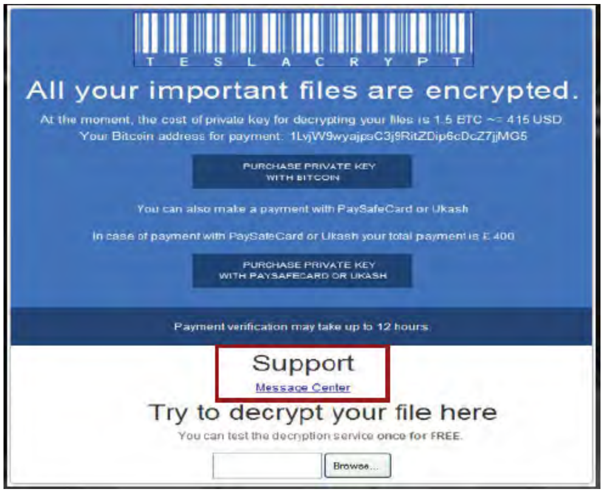
Internet of Things (IoT)

- All things physical connected to the Internet
  - ▶ Estimated 31 billion devices connected to the Internet
- New platforms create new cyber attack opportunities
  - ▶ Smart home devices (e.g., security systems, thermostats, lighting)
  - ▶ Embedded devices (e.g., DVRs, smart TVs, webcams, wireless access points, digital assistants, smartphones, printers, routers)
  - ▶ Automobiles, robotics, cloud pets, vacuum cleaners, medical devices
  - ▶ Electronic signs, HVAC

Evolution of ransomware – Dual threat

- Encrypt organization’s data and require ransom to be paid for encryption key
  - Backup for recovery as a reactive control
- Name and shame
  - Threat of leaking the organization’s data on the internet
- Average downtime of a ransomware attack is 19 days
- Extortion demands have drastically increased – many are demanding six-figure sums to release the data

Evolution of ransomware – Dual threat


TESLACRYPT
PURCHASE PRIVATE KEY WITH BITCOIN
PURCHASE PRIVATE KEY WITH PAYSAFECARD OR UKASH
Support
Message Center
Browse...

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~= 415 USD
Your Bitcoin address for payment: 1LvjW9wyajpsC3j9RitZDip6cDcZ7jjMG5

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is £ 400

Payment verification may take up to 12 hours.

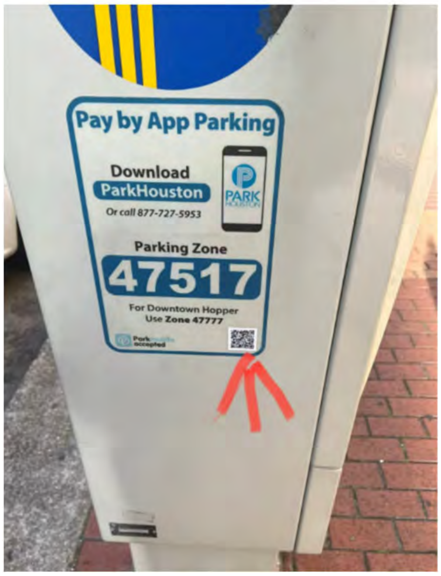
Try to decrypt your file here

You can test the decryption service once for FREE.

Crimeware-as-a-Service (CaaS)

- Cyber services for hire
  - Malicious code (Keylogger, ransomware, remote access)
  - Exploit kits
  - Distributed denial of service attacks
  - Email hacking
  - Social media account hacking

QR code phishing



QR code phishing

- One is good and one is bad… Do you know the difference?

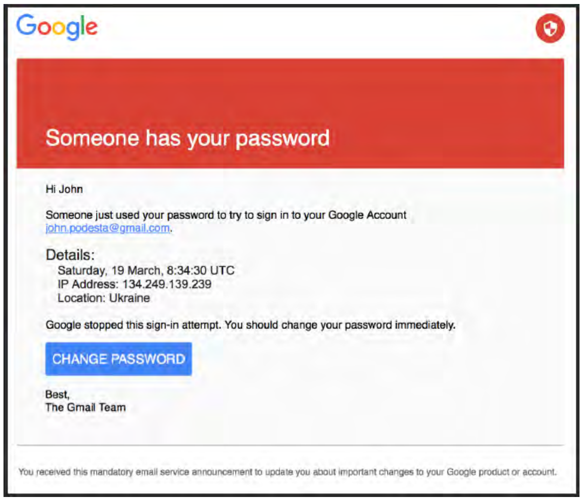
QR code phishing

- Treat them the same way as links in emails.
  - Is it taking you to a website you were expecting? Does it look as it should?
  - Use a clean browser and type in the web address manually before logging in or making a payment
- Think before you scan. Is it a sticker? Is it in an email?
- A password manager can be helpful to spot websites that do not represent the legitimate site.
- Use QR code scanning apps that filter phishing sites.

Case Study

Credential Harvesting

Case study – Targeted phishing attack



Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

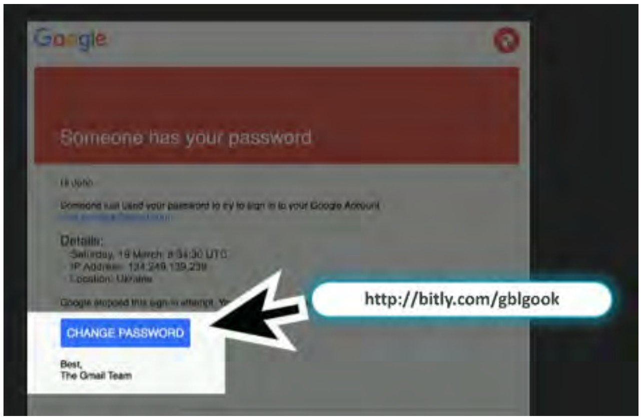
Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

Case study – Targeted phishing attack



Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. Yo

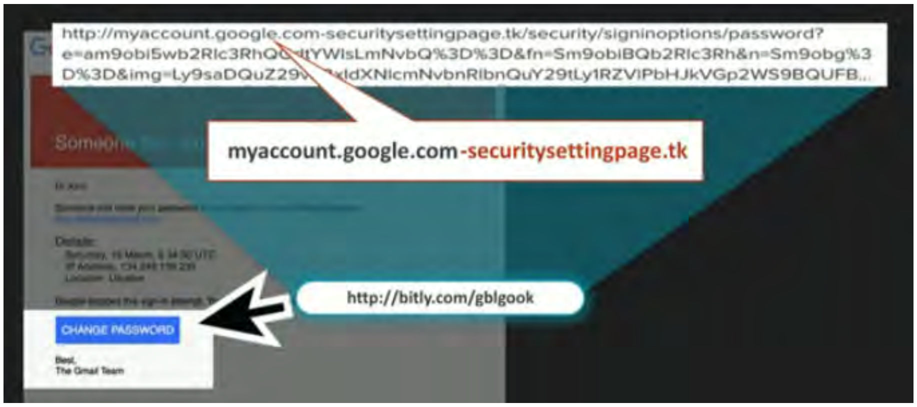
CHANGE PASSWORD

Best,
The Gmail Team

http://bitly.com/gblgook

Shortened URL

Case study – Targeted phishing attack



http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?
e=am9obi5wb2Rlc3RhQG dtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3
D%3D&img=Ly9saDQuZ29v xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFB...

myaccount.google.com-securitysettingpage.tk

http://bitly.com/gblgook

Someone

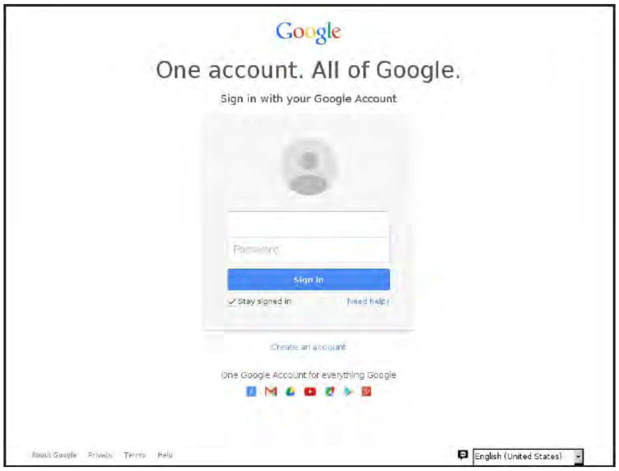
Hi John

Details:

CHANGE PASSWORD

Best,
The Gmail Team

Case study – Targeted phishing attack



One account. All of Google.

Sign in with your Google Account

Fake Google Website

Case Study

Russian cyber attacks against Ukraine

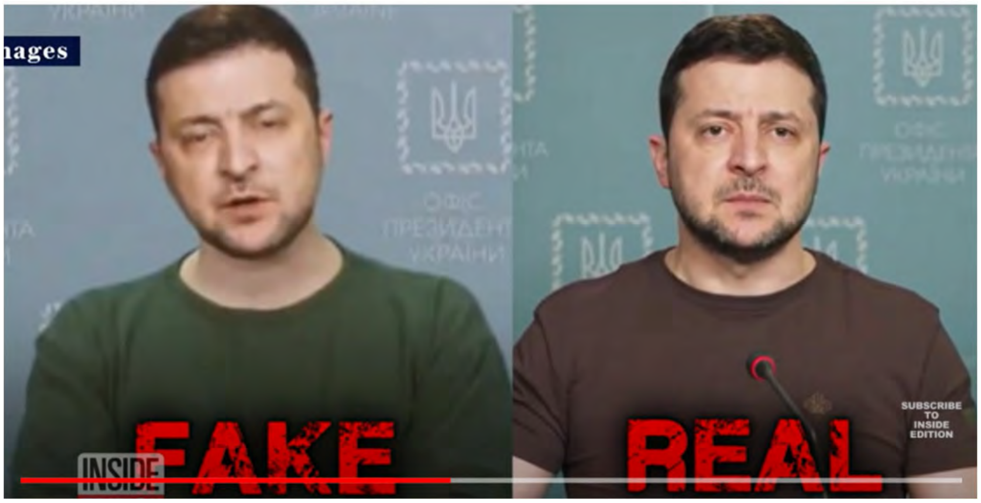
Russia cyber attacks against Ukraine – Targets

- Government websites
- Critical infrastructure
  - Transportation
  - Financial Services
  - Utilities – energy, gas, oil
  - Communications
  - Many others
- President Biden warns of U.S. cyber attacks

Russia cyber attacks against Ukraine – Attack types

- Misinformation
  - Social media
  - Deep fake videos
- Wiper malware
  - Erases and destroys data
- DDoS attacks

Deepfake video – Misinformation



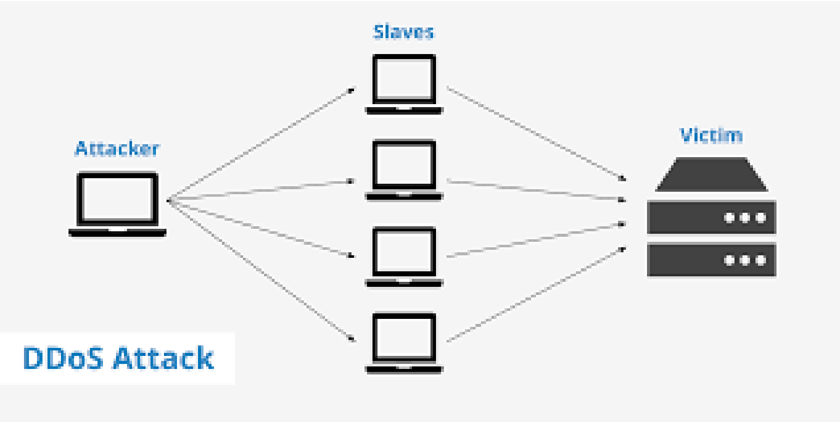
Wiper malware

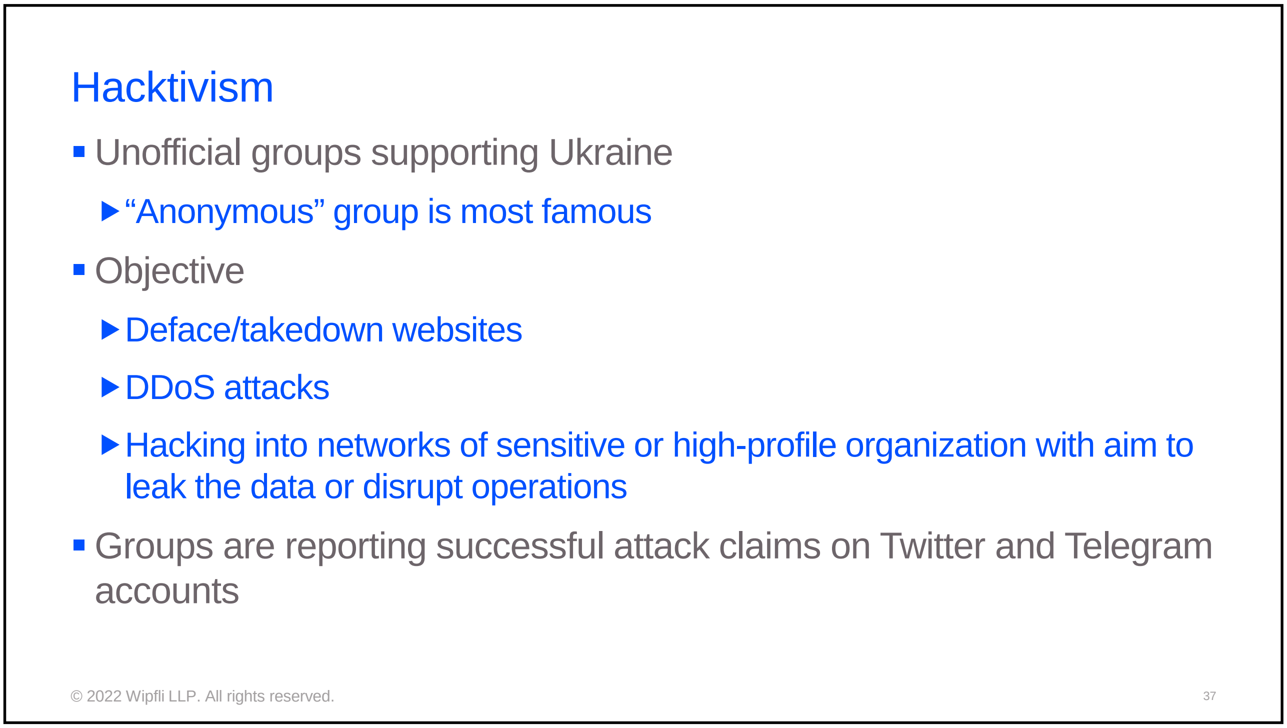
- Wiper malware used against Ukraine included CaddyWiper, HermeticWiper, and IsaacWiper
- Erases data
- Corrupts hard drive partition by damaging boot partition

Distributed Denial of Service (DDoS)

- Traditionally has been used for extortion
  - ▶ Becoming one of the top threats for financial institutions
- Sabotage through disruption
  - ▶ Power plants and other critical infrastructure
- Very difficult to defend against

Distributed Denial of Service (DDoS)



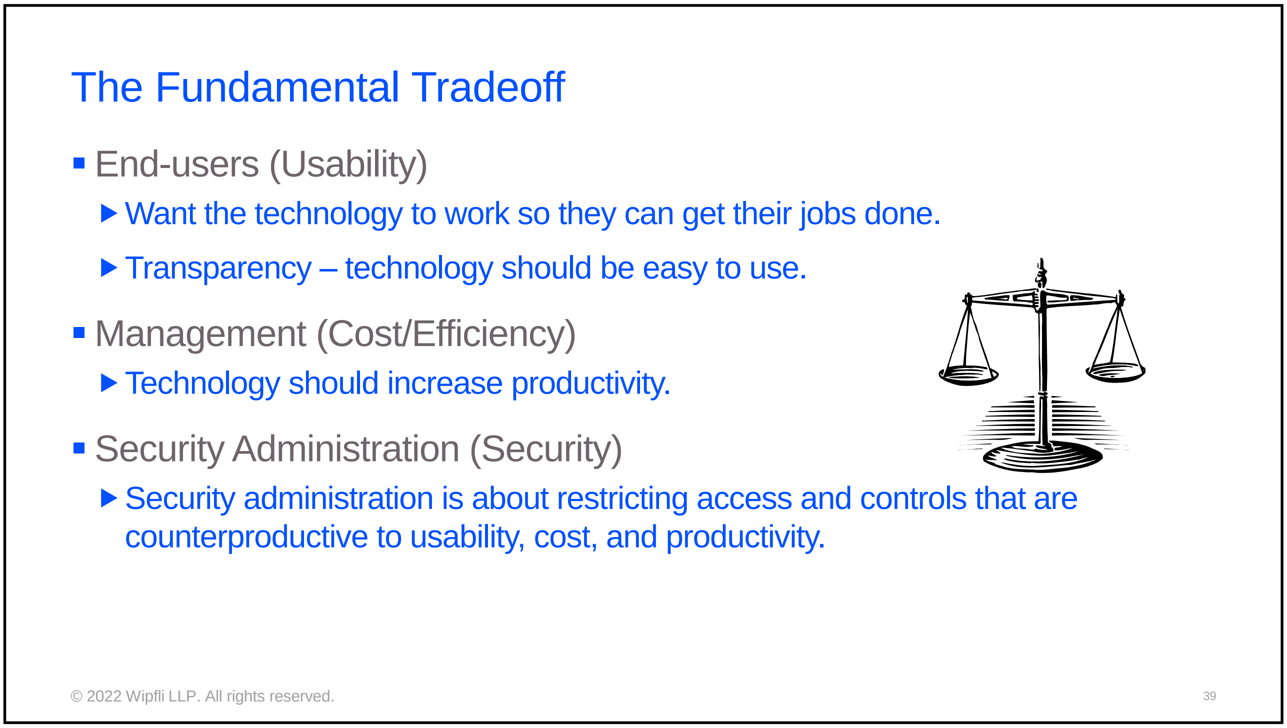


Hacktivism

- Unofficial groups supporting Ukraine
  - “Anonymous” group is most famous
- Objective
  - Deface/takedown websites
  - DDoS attacks
  - Hacking into networks of sensitive or high-profile organization with aim to leak the data or disrupt operations
- Groups are reporting successful attack claims on Twitter and Telegram accounts

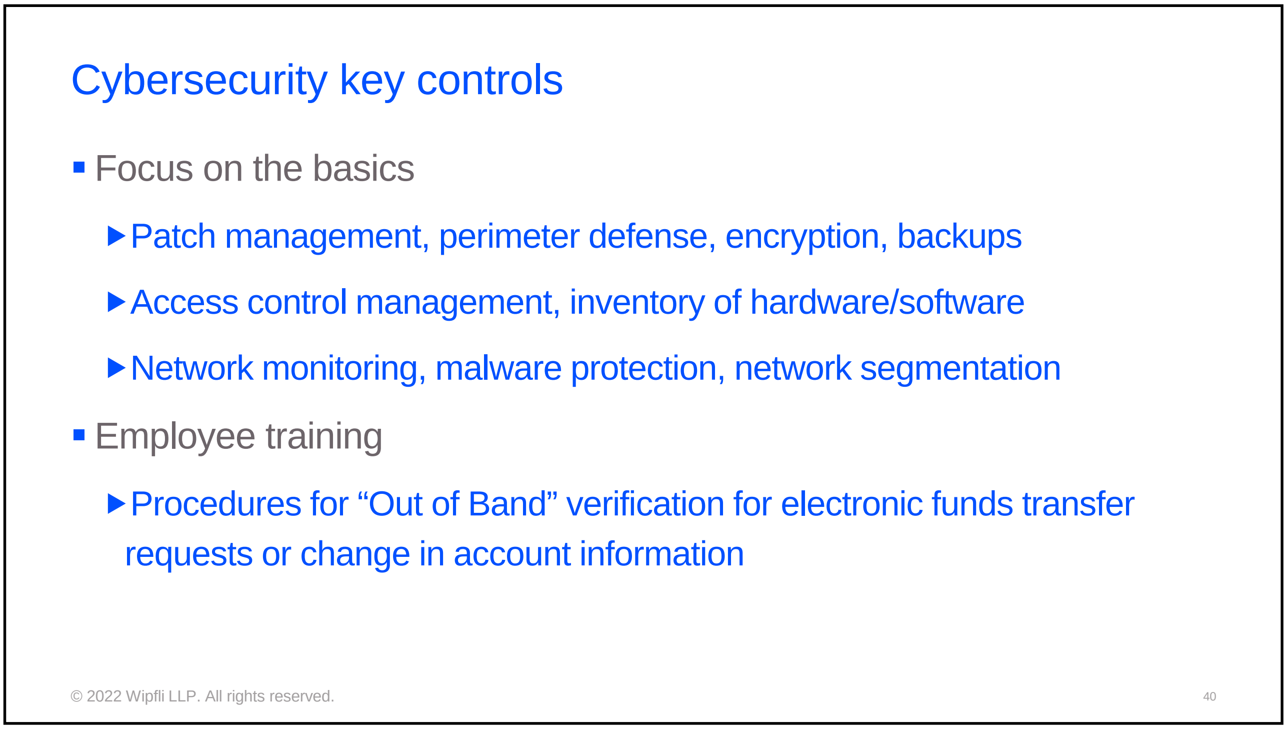
Risk Management

Key Controls



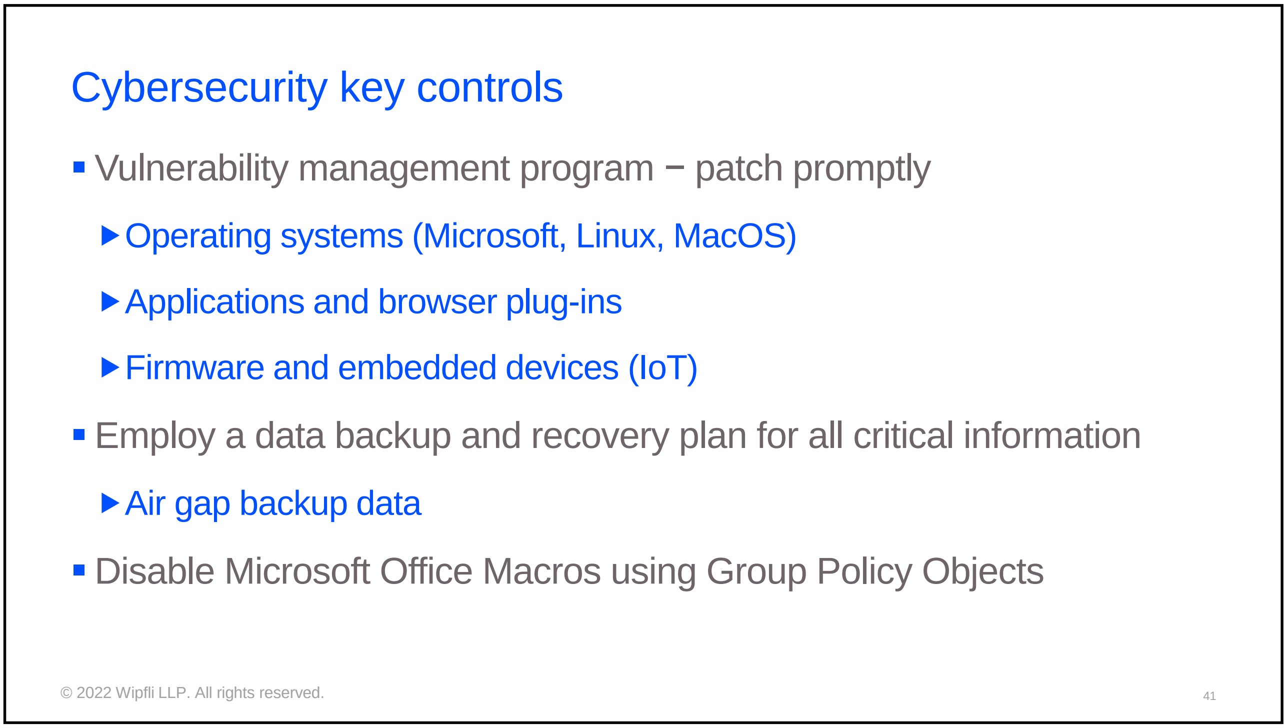
The Fundamental Tradeoff

- End-users (Usability)
  - Want the technology to work so they can get their jobs done.
  - Transparency – technology should be easy to use.
- Management (Cost/Efficiency)
  - Technology should increase productivity.
- Security Administration (Security)
  - Security administration is about restricting access and controls that are counterproductive to usability, cost, and productivity.



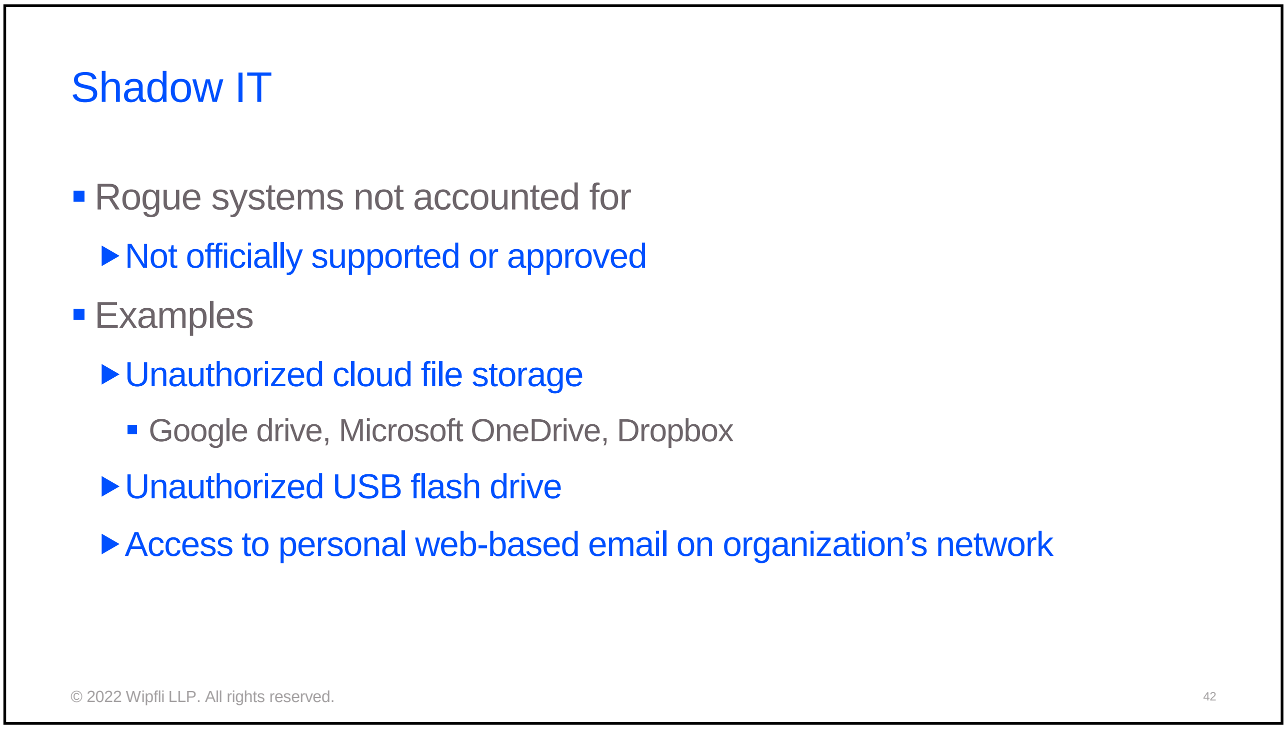
Cybersecurity key controls

- Focus on the basics
  - Patch management, perimeter defense, encryption, backups
  - Access control management, inventory of hardware/software
  - Network monitoring, malware protection, network segmentation
- Employee training
  - Procedures for “Out of Band” verification for electronic funds transfer requests or change in account information



Cybersecurity key controls

- Vulnerability management program − patch promptly
  - ▶ Operating systems (Microsoft, Linux, MacOS)
  - ▶ Applications and browser plug-ins
  - ▶ Firmware and embedded devices (IoT)
- Employ a data backup and recovery plan for all critical information
  - ▶ Air gap backup data
- Disable Microsoft Office Macros using Group Policy Objects



Shadow IT

- Rogue systems not accounted for
  - ▶ Not officially supported or approved
- Examples
  - ▶ Unauthorized cloud file storage
    - Google drive, Microsoft OneDrive, Dropbox
  - ▶ Unauthorized USB flash drive
  - ▶ Access to personal web-based email on organization’s network

Strong authentication – Passwords

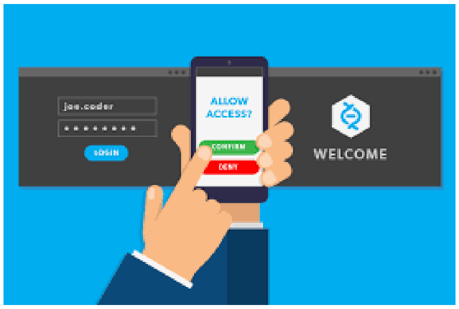
- Hackers continue to use stolen and/or weak passwords
  - ▶ Default credentials
  - ▶ Common passwords
  - ▶ Data breaches (Yahoo, LinkedIn)
  - ▶ Malicious software (keyloggers)
  - ▶ Tricking victims to disclose password
- Adding two numbers to the end of passwords does not make them stronger

Strong authentication – Passwords

- Passwords should be minimum length of 14 characters
- Password managers
  - ▶ Generates strong and unique passwords
  - ▶ Auto-fill logins
  - ▶ Provides security score for "at-risk" passwords
  - ▶ Notifies you of any login credentials involved in a data breach
  - ▶ Synch across devices

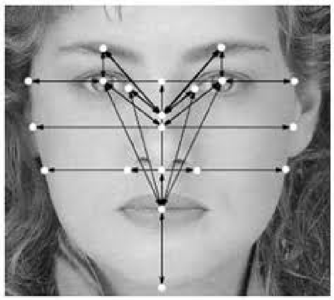
Strong authentication

- Multi-factor authentication
  - Incorporates two of three
    - What you know
    - What you have
    - Who you are
  - Implementation
    - All remote access (VPN, OWA, etc.)
    - Administrative accounts
    - All accounts???



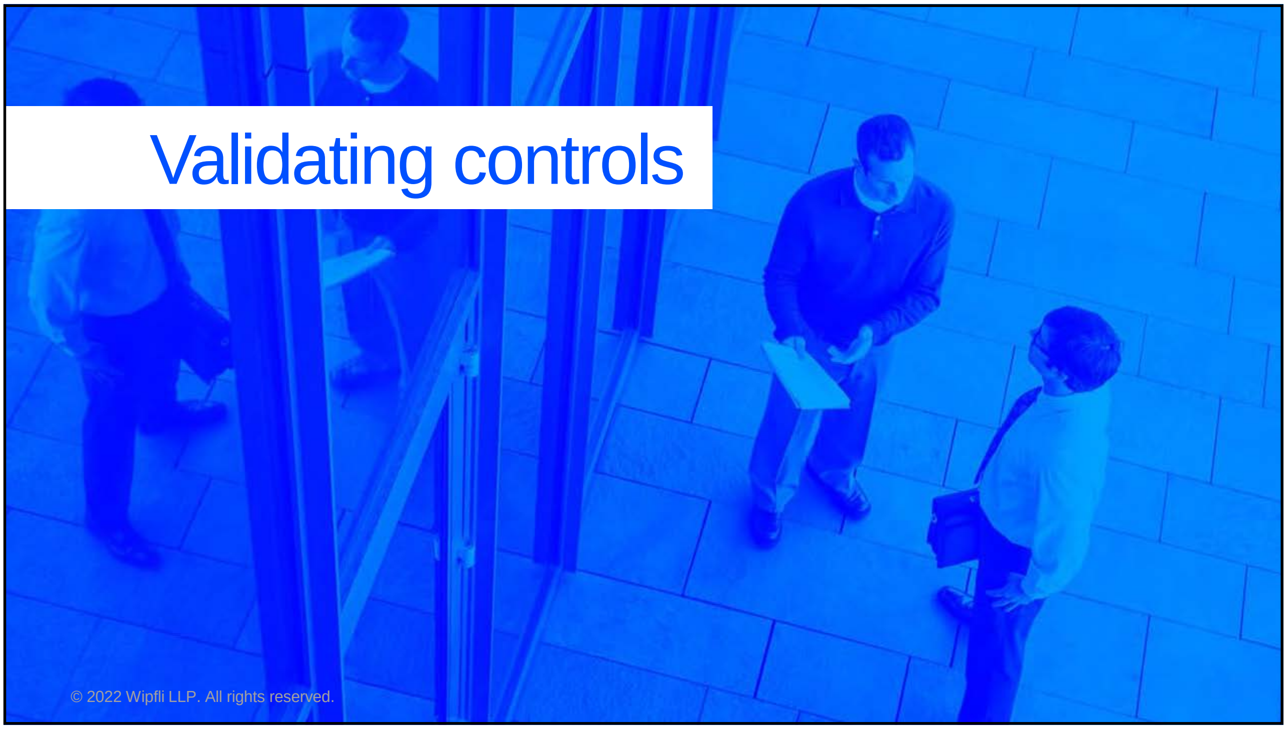
Strong authentication – Biometrics

- Biometric authentication
  - Fingerprint scanning
  - Voice recognition (yuk!)
  - Facial pattern recognition
  - Iris scanning
  - Contactless palm scanning



Employee training

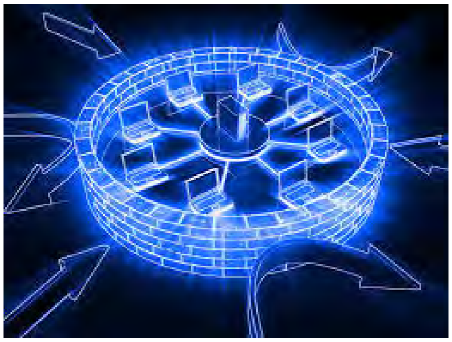
- Understand safeguards
- Incident response
  - When and how to respond to an incident
  - Who to report the incident
- Ongoing training works best



Validating controls

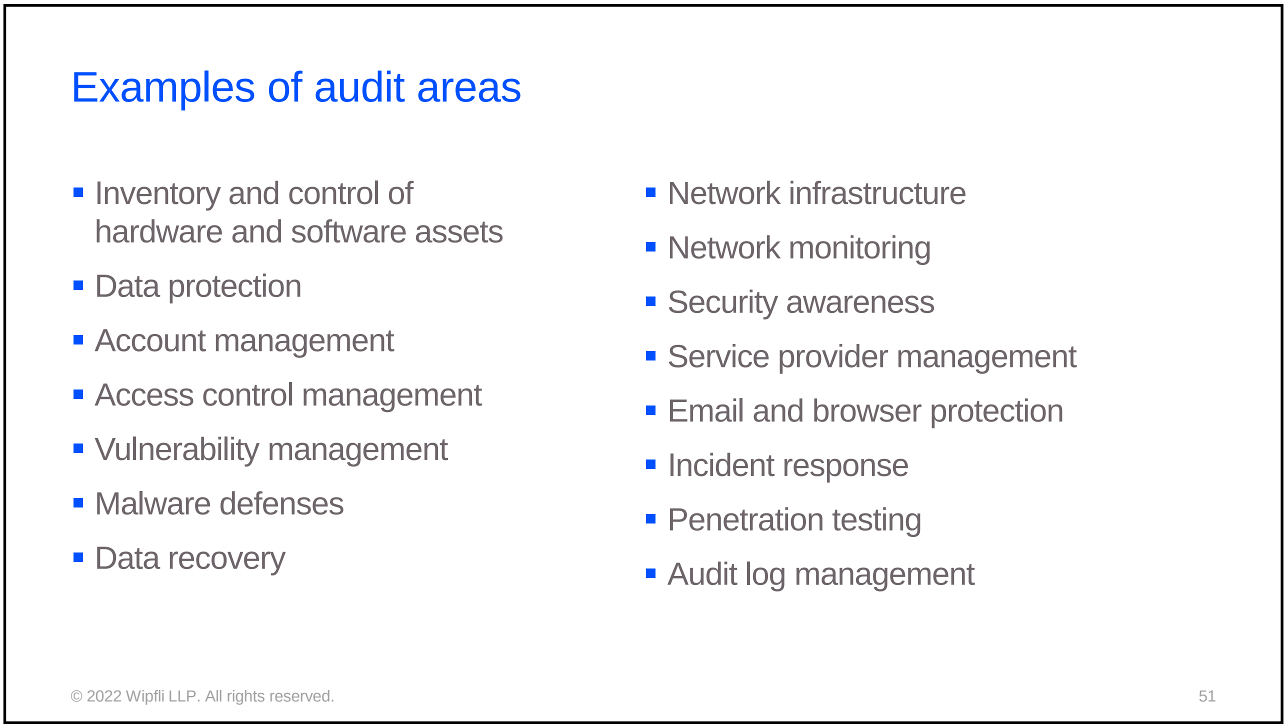
Validating your controls

- IT general controls review
- Penetration tests
- Vulnerability assessments
- Cloud security assessments
  - M365, AWS, Azure
- Social engineering
  - Email spoofing
  - Pretext calling
  - Onsite physical pen testing



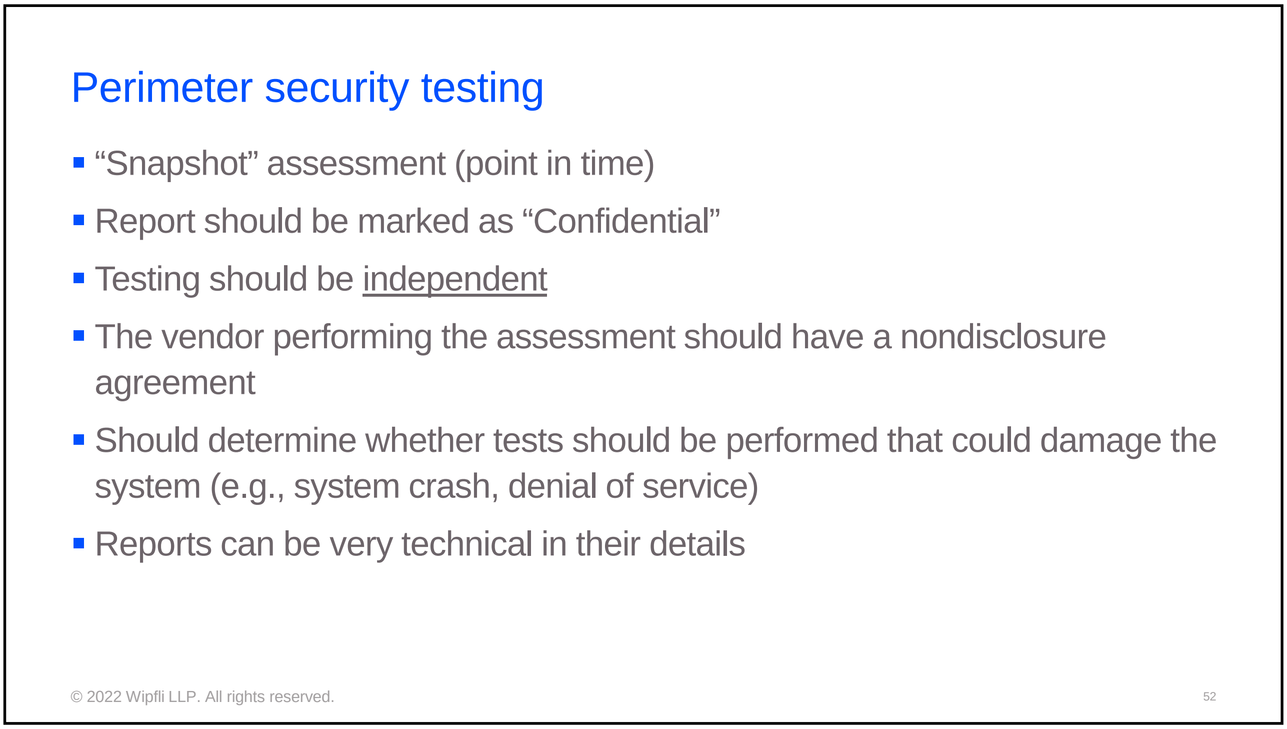
IT audit frameworks

- Adds focus, credibility, and consistency to the IT audit process
- Common IT frameworks:
  - CIS Top 18 critical security controls
    - https://www.cisecurity.org/controls/cis-controls-list
  - NIST 800-53
    - www.nist.gov
  - COBIT
    - www.isaca.org



Examples of audit areas

- Inventory and control of hardware and software assets
- Data protection
- Account management
- Access control management
- Vulnerability management
- Malware defenses
- Data recovery
- Network infrastructure
- Network monitoring
- Security awareness
- Service provider management
- Email and browser protection
- Incident response
- Penetration testing
- Audit log management



Perimeter security testing

- “Snapshot” assessment (point in time)
- Report should be marked as “Confidential”
- Testing should be independent
- The vendor performing the assessment should have a nondisclosure agreement
- Should determine whether tests should be performed that could damage the system (e.g., system crash, denial of service)
- Reports can be very technical in their details

Vulnerability scanning vs. penetration testing

Vulnerability scan

- More automated
- Comprehensive and not meant to be "stealthy"
- Involves both simple and sophisticated scanning tools
- Results may show "false positives"
- The objective is not to eliminate all vulnerabilities

Penetration test

- Rules of engagement should be defined – can include both technical and non-technical methods
- Goal-oriented, focused
- Typically, time-based
- Attempts to exploit vulnerabilities
- Requires expertise – web, network infrastructure, other
- Involves toolsets and manual techniques

Internal network scanning

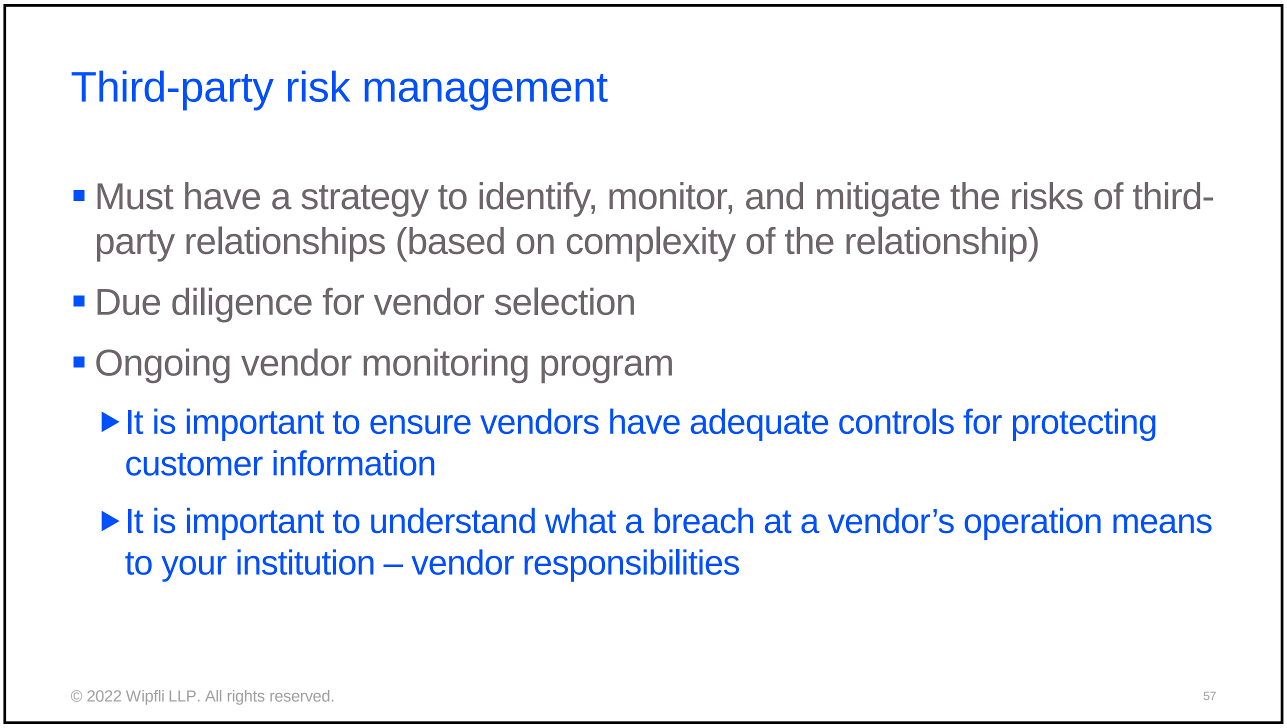
- Scans for internal system vulnerabilities
  - Can show security configuration weaknesses (e.g., default passwords, weak parameter settings)
  - Identify "unpatched"/unsupported systems and applications
  - Discover rogue applications
  - "Credential scans" can provide even more detailed results

Social engineering testing

- Both technical and nontechnical attacks
  - Trend: People are the targets, not the systems
- Typically performed using:
  - Electronic mail (e.g., spam, phishing, whaling)
  - Telephone/Pretext calling
  - Physical entry
- Preys on human nature
- Invented scenario (the pretext)

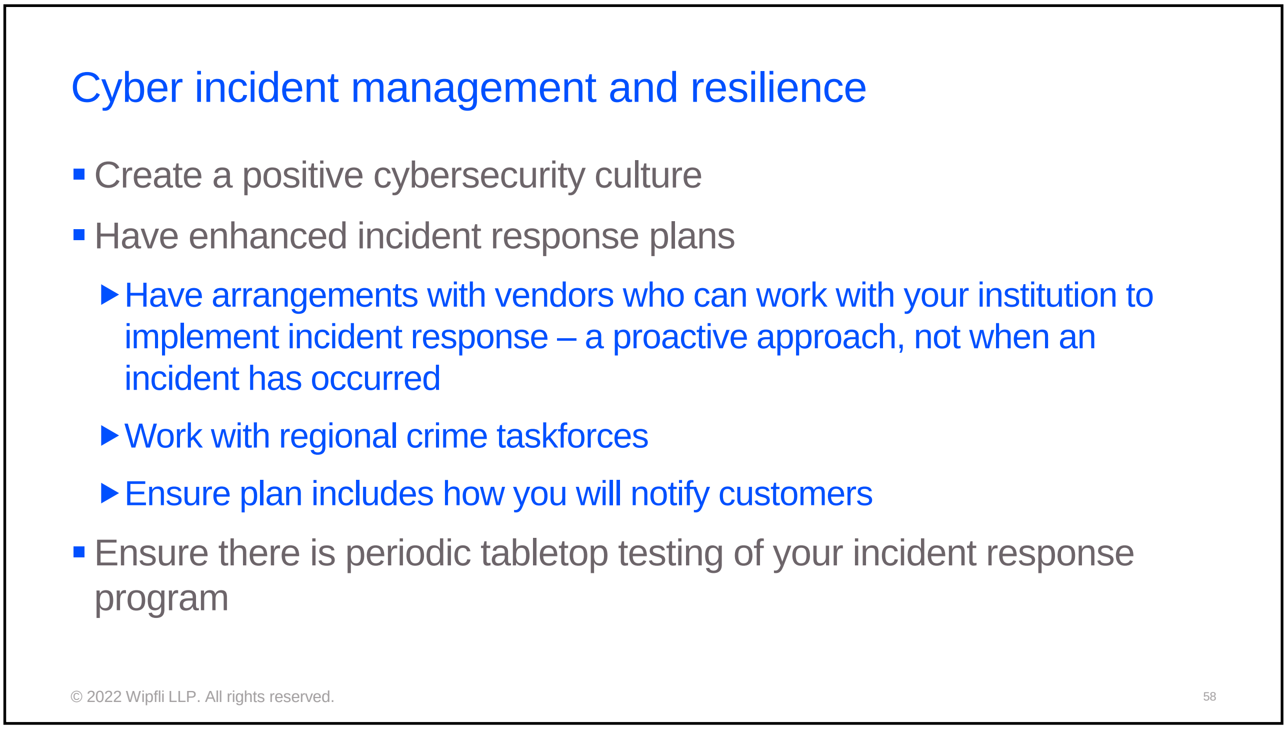
Risk management and oversight

- Board involvement!!! Ensure cybersecurity moves from the backroom to the boardroom
  - Is the Board updated on cybersecurity issues?
  - Does the Board understand how you are mitigating cyber threats?
  - Make “cybersecurity” a standing agenda item for IT committee, audit committee, and Board meetings
  - Involve the Board members in IT committee meetings



Third-party risk management

- Must have a strategy to identify, monitor, and mitigate the risks of third-party relationships (based on complexity of the relationship)
- Due diligence for vendor selection
- Ongoing vendor monitoring program
  - It is important to ensure vendors have adequate controls for protecting customer information
  - It is important to understand what a breach at a vendor's operation means to your institution – vendor responsibilities



Cyber incident management and resilience

- Create a positive cybersecurity culture
- Have enhanced incident response plans
  - Have arrangements with vendors who can work with your institution to implement incident response – a proactive approach, not when an incident has occurred
  - Work with regional crime taskforces
  - Ensure plan includes how you will notify customers
- Ensure there is periodic tabletop testing of your incident response program

Cybersecurity insurance

- Fee is increasing mostly due to ransomware attacks (74%???)
  - Drastic increase in extortion demands
  - Mandated notifications
- No more blanket coverage
  - Multi-factor authentication
  - Security monitoring
  - Other established safeguards
- Pay attention to exclusionary language

Resources

Cybersecurity resources

- Cybersecurity & Infrastructure Security Agency
  - Email bulletins
    - https://www.cisa.gov/uscert/mailing-lists-and-feeds
  - Shields Up
    - https://www.cisa.gov/shields-up
- 18 CIS Critical Security Controls
  - https://www.cisecurity.org/controls/cis-controls-list
- Ransomware Self-Assessment Tool
  - https://www.csbs.org/ransomware-self-assessment-tool

Audit tools

- Nessus
- DumpSec
- SolarWinds
- Nmap/Zenmap
- Windows Sysinternals
- Spiceworks
- Drlinkcheck.com
- Netwrix Auditor
- Splunk
- Kali Linux

InfraGard

- www.infragard.org
- Partnership between the FBI and members of the private sector
- Provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure

Cybersecurity threats and trends

- Threat actors are interested in you – everyone is a target
  - Small business, large business, individuals…

Questions?