

Nonprofit Conference

April 29, 2026



HASKELLWHITE

CERTIFIED PUBLIC ACCOUNTANTS | BUSINESS ADVISORS

THE VALUE OF
EXPERIENCE

Agenda

- **Welcome**
- **Ripped from the Headlines: Fraud in Nonprofits**
- **Insurance & Risk: Protecting Your Mission and Leadership**
- ***Break***
- **Navigating Common Nonprofit Accounting Challenges**
- **Right-Sized Security: Practical Cybersecurity for Nonprofits**

About Haskell & White

- **Middle-market** focused accounting and advisory firm with Irvine and San Diego offices, a remote workforce and backed by a global alliance of firms
- A **great** place to work and corporate **role model**
- **Technical competencies** and **experience** of larger firms combined with the **attentiveness** and **responsiveness** of smaller firms
- Serve the nonprofit community by providing audits, single audits, 990 preparation and other services that we provide with a reasonable fee structure. More value for your fee dollars
- Serve private and public companies with revenues up to \$700 million with audit, tax and advisory services in a variety of industries, including: real estate, technology, life science, manufacturing and distributing, and nonprofit
- Proud legacy of excellent AICPA Peer Review reports



Hybrid Session and CPE



Keep your audio on mute to limit background noise for other virtual attendees



Send questions via Zoom's chat feature



On Zoom answer the poll questions (5 out of 7 need to be answered to get CPE!)



Zoom Attendees will receive certificate via email



May not be applicable in all states



Presenters



Wayne Pinnell, CPA
Managing Partner
wpinnell@hwcpa.com



Rick Smetanka, CPA
Audit Partner-in-Charge
rsmetanka@hwcpa.com



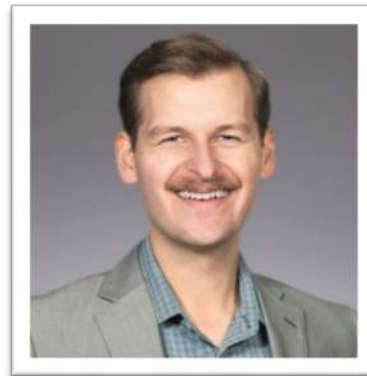
Diane Wittenberg, CPA
Audit Partner
dwittenberg@hwcpa.com



Pat Ross, CPA
Audit Partner
pross@hwcpa.com



David Brownstein, CPA
Audit Partner
dbrownstein@hwcpa.com



Spencer Giles, CISSP, GSNA
IT Assurance Senior Manager and
Information Security Officer
sgiles@hwcpa.com



Michael Fitch, ARM, CIC
Vice President
HUB International
Michael.Fitch@hubinternational.com

Ripped from the Headlines: Lessons Learned from Nonprofit Fraud Cases

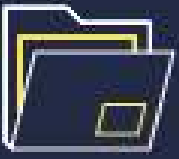




Polling Question #1

How much do Organizations worldwide lose to fraud each year?

- A. \$20 trillion
- B. \$5 trillion
- C. \$100 billion
- D. \$50 billion



1,921
CASES

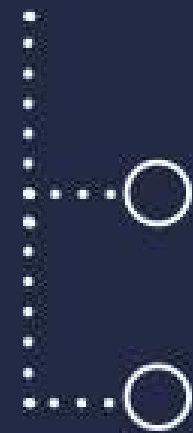
from



138
COUNTRIES and
TERRITORIES

Causing total
losses of more than

\$3.1 BILLION



\$1,662,000

Average loss per case



22% of cases had losses of
\$1 million+

CFEs estimate that
organizations **LOSE**



5% of revenue
to **FRAUD**
each year

Projected against
2022 GWP*
(\$101 TRILLION)

that's more than
\$5 TRILLION
LOST TO FRAUD
GLOBALLY

[*https://databank.worldbank.org/data/download/GDP.pdf](https://databank.worldbank.org/data/download/GDP.pdf)

Highlights from the Association of Certified Fraud Examiners
2024 Report to the Nations (the largest global study on
occupational fraud).

Fraud is Big Business

FIG. 13 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?

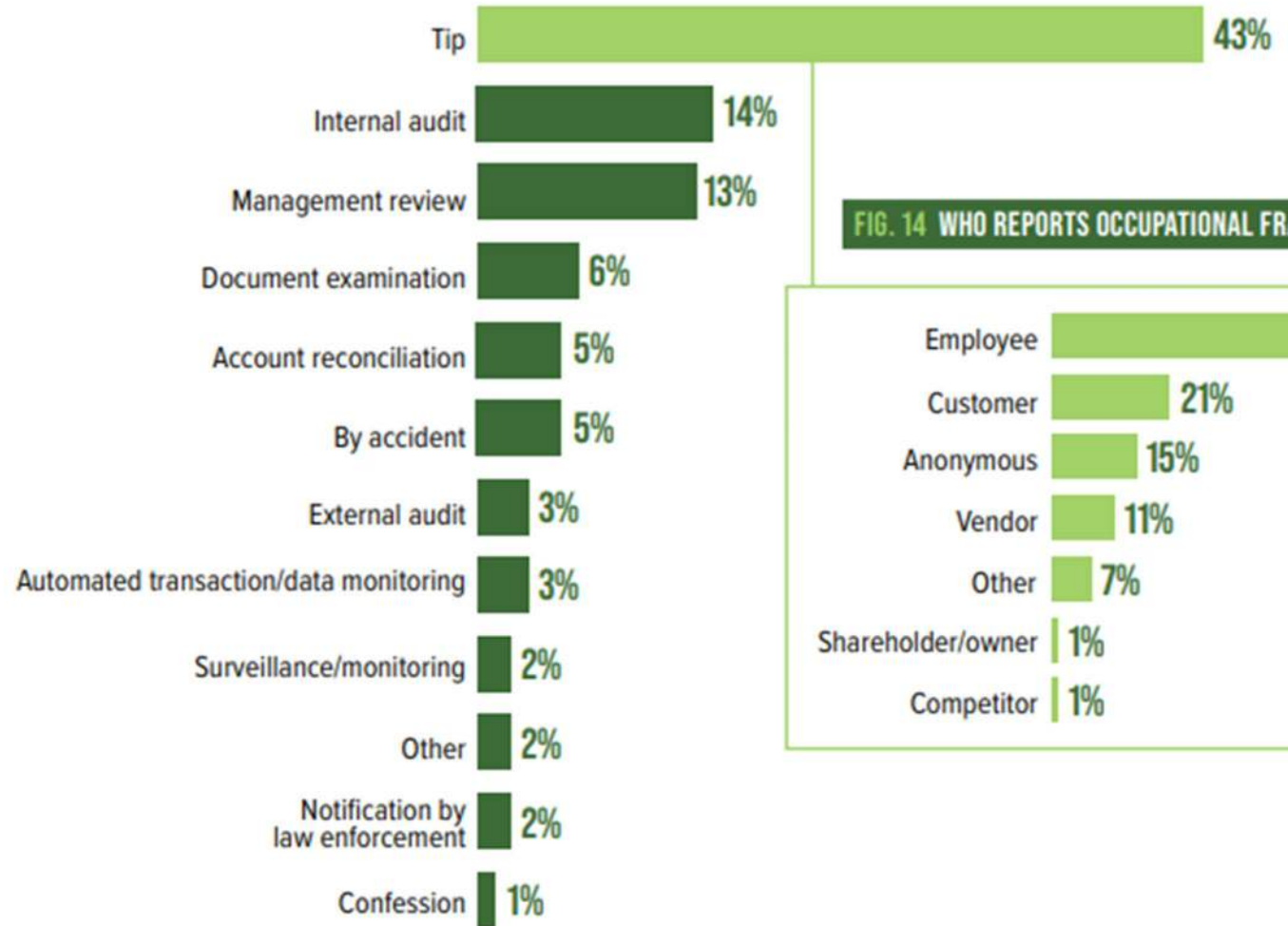
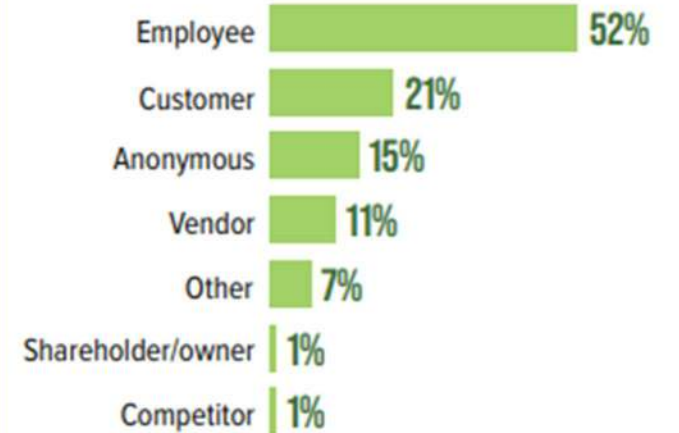


FIG. 14 WHO REPORTS OCCUPATIONAL FRAUD?

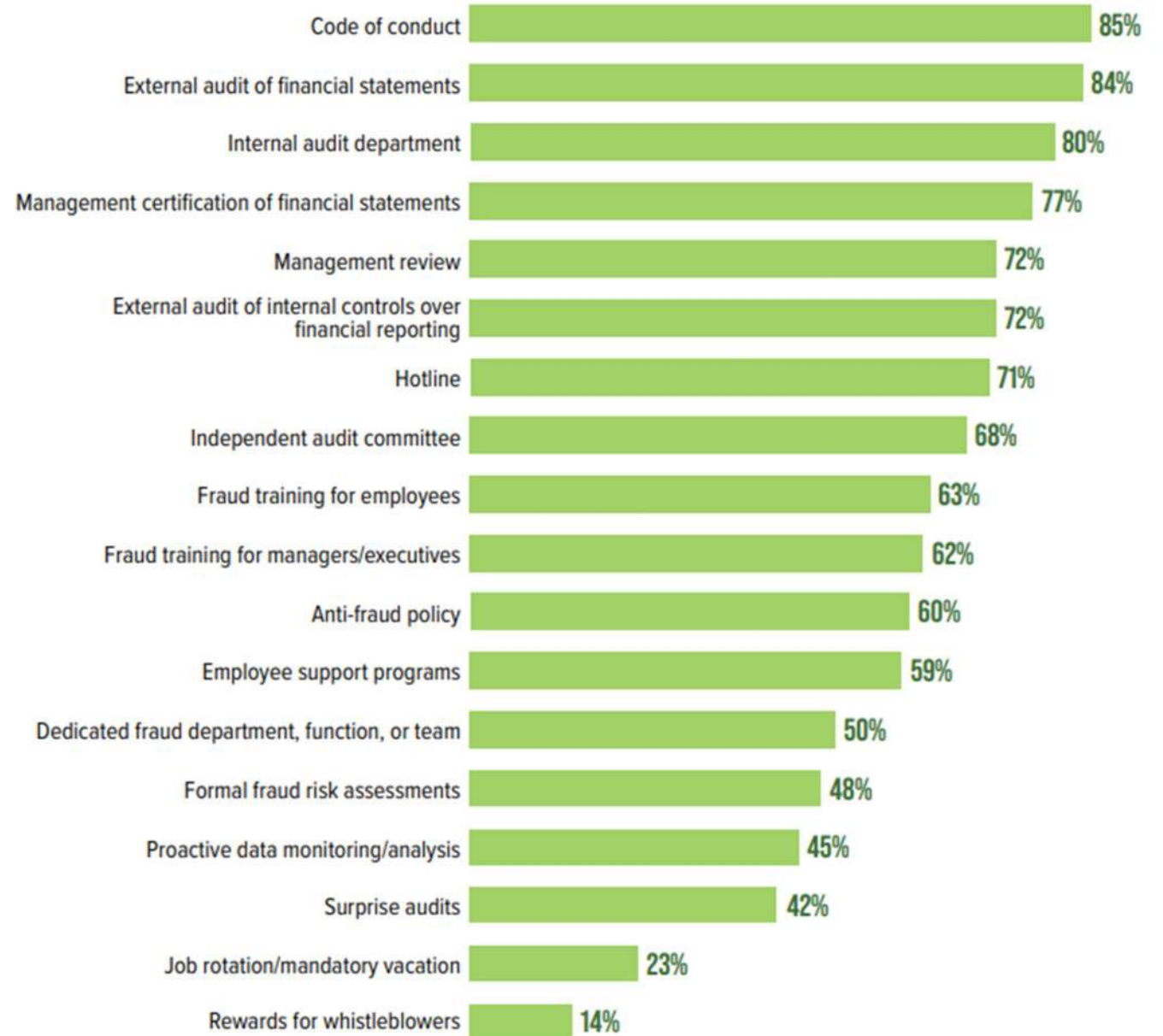


Highlights from the Association of Certified Fraud Examiners 2024 Report to the Nations (the largest global study on occupational fraud).

Fraud is Big Business

Highlights from the Association of Certified Fraud Examiners 2024 Report to the Nations (the largest global study on occupational fraud).

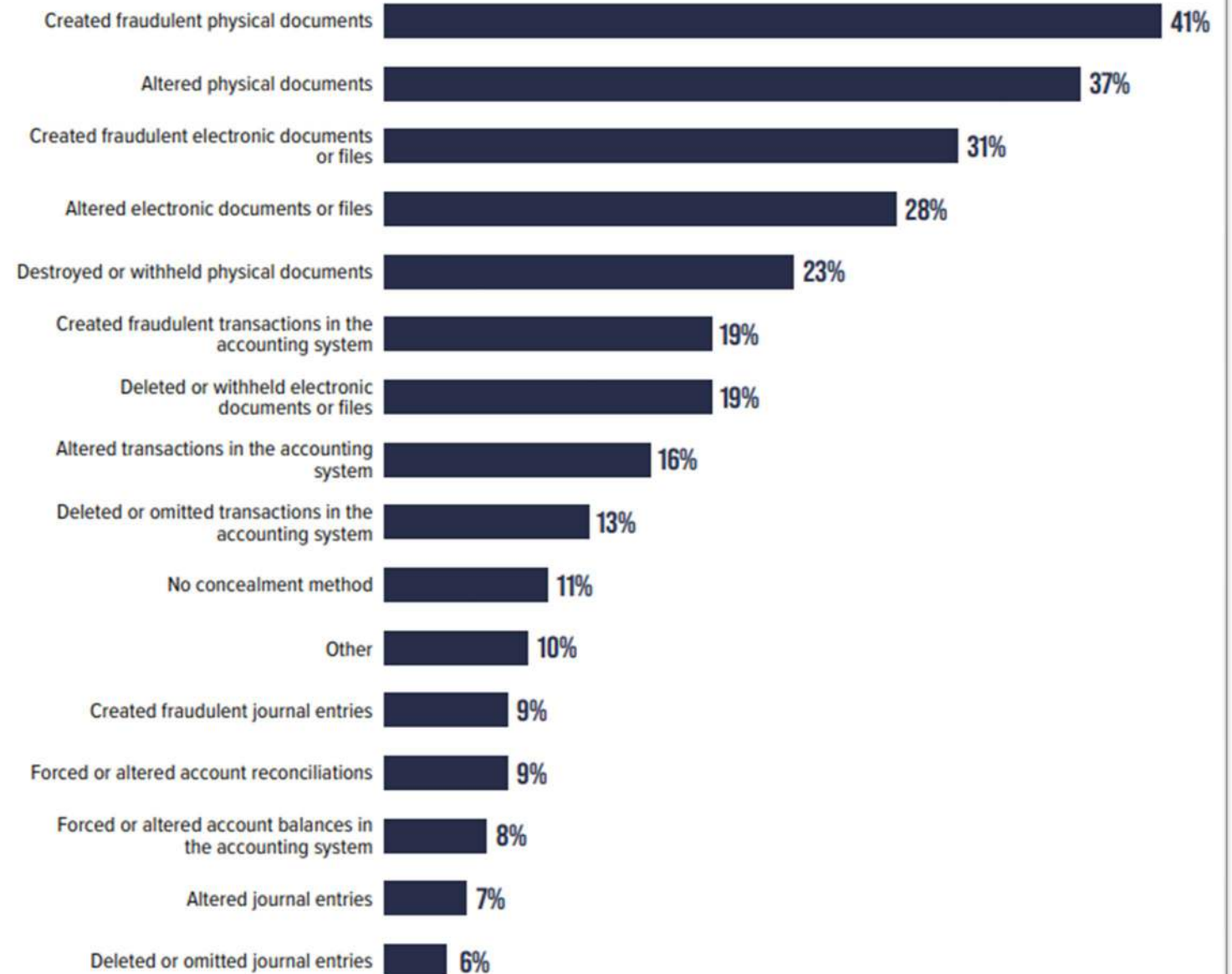
FIG. 27 WHAT ANTI-FRAUD CONTROLS ARE MOST COMMON?



Fraud is Big Business

Highlights from the Association of Certified Fraud Examiners 2024 Report to the Nations (the largest global study on occupational fraud).

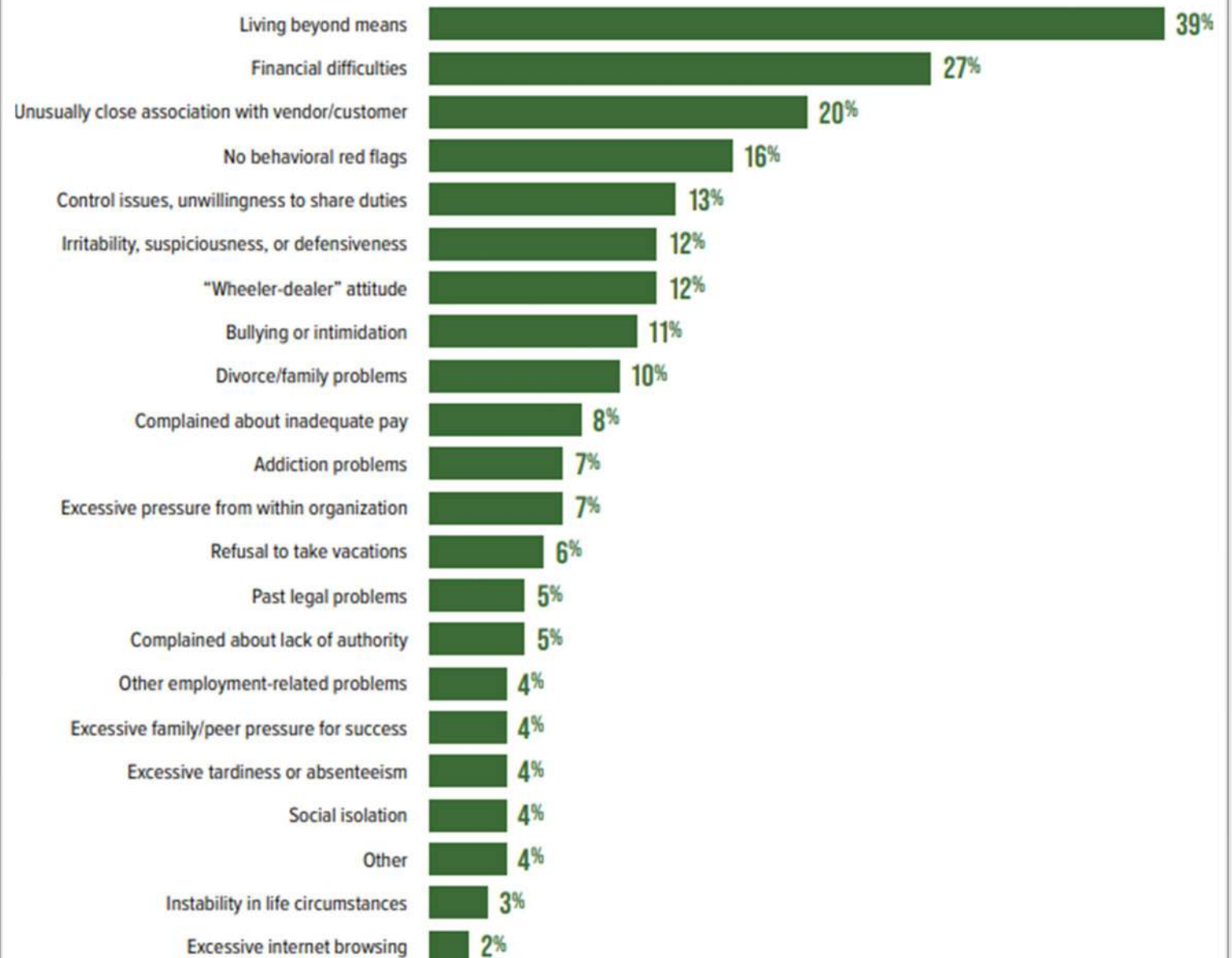
FIG. 10 HOW DO OCCUPATIONAL FRAUDSTERS CONCEAL THEIR SCHEMES?



Fraud is Big Business

Highlights from the Association of Certified Fraud Examiners 2024 Report to the Nations (the largest global study on occupational fraud).

FIG. 54 HOW OFTEN DO PERPETRATORS EXHIBIT BEHAVIORAL RED FLAGS?



Case 1: Detroit Riverfront Conservancy

About Detroit Riverfront Conservancy (DRC)

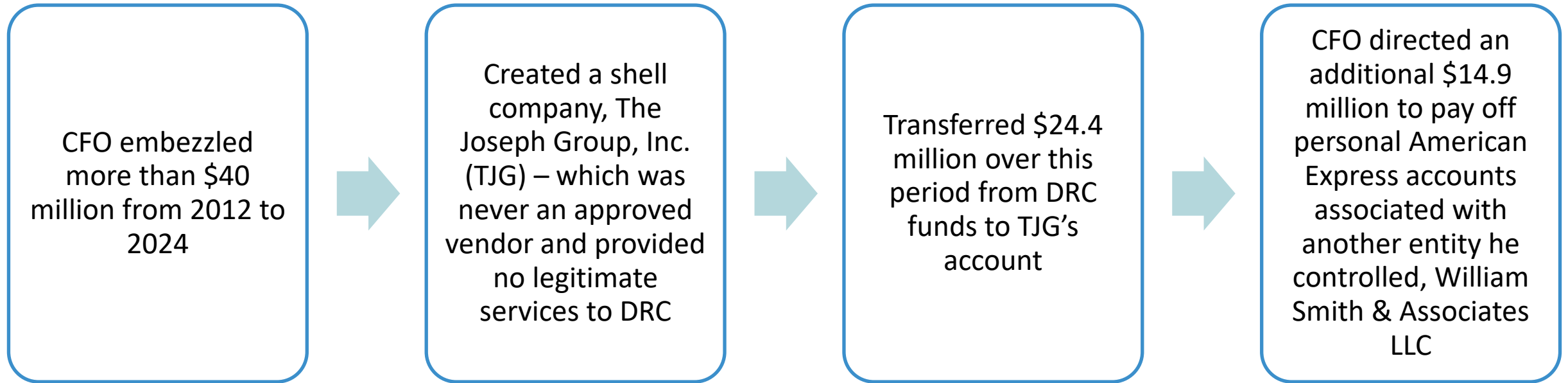
- Mission of developing and enhancing public access to Detroit's riverfront
- Revitalization of the riverfront includes vibrant green space, plazas, parks, and a continuous riverwalk that stretches across the city
- Annual revenue of approximately \$39M, funded through private donations and public grants
- William Smith was the CFO from 2011 through 2024





Case 1: Detroit Riverfront Conservancy – What Happened

Shell Companies





Case 1: Detroit Riverfront Conservancy – What Happened

Falsifying Documents

- CFO falsified bank statements provided to DRC's bookkeeper by removing unauthorized transfers so they would not be reflected in the accounting records
- Falsified bank statements allowed the fraud to remain hidden for 12 years
- CFO also obtained a \$5 million line of credit in DRC's name by providing forged authorization documents
- Used the \$5 million to inject cash back into DRC's bank accounts to obscure the extent of his theft





Case 1: Detroit Riverfront Conservancy - What Went Wrong

- CFO had exclusive control over DRC's bank accounts, access to online banking credentials, sole discretion in executing transfers, ability to make financial decisions without meaningful oversight
- There was no dual authorization process or independent read-only access for another executive, board member, or finance committee member
- Combination of CFO's long tenure and control insulated his activities from scrutiny
- Board relied heavily on management-prepared reports; its review of financials was high-level and not sufficiently detailed
- No procedures to verify the legitimacy of vendor relationships, such as TJG





Case 1: Detroit Riverfront Conservancy

Impact of the Fraud

Mission Delays

Funds stolen from DRC meant fewer resources for riverfront development and park projects, forcing delays in planned segments of the Riverwalk and other initiatives.

Leadership

The scandal prompted the resignation of the DRC's CEO and a change in its external auditing firm — signaling a shake-up in governance and accountability practices. The CFO was terminated and eventually sentenced to 19 years in prison.

Reputational Harm

The reputational damage to DRC was significant, undermining donor confidence and public trust in one of Detroit's most visible civic organizations. In 2024, DRC's annual revenue declined to \$38.9 million, down from \$52.1 million in 2023.

Reforms

In response, the organization has undertaken governance reforms, including reducing board size, imposing term limits, outsourcing certain financial functions, and strengthening transaction oversight and risk management — highlighting a commitment to rebuild trust and prevent future breakdowns.



Case 1: Detroit Riverfront Conservancy – Lessons Learned

Segregate Duties

No single person should have control over banking, payments, reconciliation, and financial reporting. Segregation of duties is essential to prevent misuse of funds.

Independent Access and Verification

Ensure that multiple people — such as the treasurer, audit chair, or an outsourced accountant — have access to financial systems.

Vendor and Transaction Controls

Establish rigorous vendor approval processes and periodic reviews of recurring and large transactions. Investigate any vendor that does not provide clear documentation of services.

Strengthen Governance

Active and financially literate boards are crucial. Boards should demand regular financial statements, ask probing questions, and be trained to understand financial reports rather than treating them as routine.

Whistleblowers Are Effective

Individuals in DRC's leadership became concerned about the accuracy of financial reports prepared by the CFO and brought those concerns to the board's attention.



Polling Question #2

How many of you have heard about the Abundant Blessings fraud case?

- A. I know all about it
- B. I've heard a little about it, but not the details
- C. I've never heard of that Organization

Case 2: Abundant Blessings

A photograph showing several volunteers in blue t-shirts working in a kitchen or food preparation area. One volunteer in the foreground is pouring water from a large metal pitcher into a clear plastic bottle. Another volunteer is holding a white takeout container with food. In the background, there are stacks of metal cups and bowls. In the foreground, there are several cardboard crates filled with fresh produce, including apples, bananas, and bread rolls.

About Abundant Blessings (AB)

- Located in Hyde Park, CA, its mission is helping people experiencing homelessness – providing housing, meals, and support services to a vulnerable population
- Annual revenue of approximately \$3M, funded through government contracts and public funding
- Alexander Soofer was the Executive Director (ED) from 2018 through 2025
- AB was supposedly providing housing units, three meals a day, and case management to hundreds of people who were unhoused or at risk



Case 2: Abundant Blessings – What Happened



Falsifying Documents and Related Party Transactions

- From 2018-2025 AB received approximately \$23 million in public funding, of which the ED diverted over \$10 million for personal use
- ED's reported salary in the latest Form 990 filing was \$145,500
- ED purchased a \$7 million home in Westwood, CA, a \$125,000 Range Rover, designer clothing, private jet travel, stays at high-end resorts, and private school tuition for his children
- ED provided falsified invoices and documents to LA Homeless Services Authority (LAHSA) and other government funders, making it appear that AB was fulfilling its contractual obligations when, in reality, many of the services were never provided
- ED engaged in related party transactions designed to conceal his diversion of funds. For example, arranging to rent properties for homeless participants at inflated prices from entities he controlled, effectively diverting nonprofit funds into his own accounts



Case 2: Abundant Blessings – What Happened

Fictitious Board and Misrepresentation of Services Provided



ED told investigators that AB's Board authorized and reviewed expenditures. However, authorities found that the Board was largely fictitious – some purported members did not exist, while others had never heard of AB.



While Abundant Blessings was contracted to provide housing and three nutritious meals a day to more than 600 participants, investigators found that participants were often served inexpensive, low-nutrient food items such as ramen noodles, canned beans, and breakfast bars — far below contractual standards. This discrepancy between reporting and reality helped mask the diversion of funds.



Case 2: Abundant Blessings – What Went Wrong

- **Lack of Board Oversight:** Board members were either fictitious, or unaware of their supposed roles. There was no evidence of board oversight of financial reporting.
- **Inadequate Segregation of Duties:** ED controlled financial reporting and contract execution. No independent review of invoices, vendor contracts, or reimbursement requests was provided.
- **Weak Contract Compliance Monitoring:** Agencies like LAHSA should require detailed compliance monitoring, including performing site visits. However, site visits were not conducted until anonymous complaints were received at the LA Controller's office in 2024. Furthermore, despite AB having more than \$2 million in revenue, no independent audit of AB's financial statements was ever performed.





Case 2: Abundant Blessings – Impact of the Fraud

Reduced Services to Vulnerable Populations

Tens of millions in public funds did not result in the contractual level of housing and nutrition services promised to homeless participants.

Erosion of Public Trust

This high-profile fraud case undermines confidence in nonprofit partners and public-funding systems meant to address critical social needs.

Regulatory and Oversight Responses

LAHSA terminated its contracts with Abundant Blessings and referred the matter to law enforcement, and local officials have called for deeper systemic reforms in homeless services funding oversight.

Potential Criminal Penalties

If convicted on federal and state charges, Soofer faces decades in prison. It's also worthy to note that Soofer's wife was listed as an officer/director in the 2024 tax return with reportable compensation of \$129,500. To date, she has not been charged with a crime.

Ceased Operations

AB ceased operations in January 2026 following the Soofer's arrest.



Case 2: Abundant Blessings – Lessons Learned

True Accountability is Essential

A board must do more than rubber-stamp decisions — it must independently review financials and ensure governance structures are real. Regular board education in financial oversight is critical.

Contract Monitoring Must Be Rigorous

Public funders should require periodic monitoring of performance data, including site visits and independent audits when applicable.

Segregation of Duties Protects Against Misconduct






No single individual should control both financial reporting and service delivery oversight. Shared authority, reviews, and cross-checks reduce opportunities for fraud.

Always Verify Third-Party Vendors

Fictitious vendors were a key element of this fraud. Nonprofits must verify vendor legitimacy, ownership, and service delivery through independent means.



Strategies to Identify Risk and Mitigate Risk

-  Cash controls (checks; electronic payments)
-  Payroll
-  Manual journal entries
-  Cyber (phishing; spoofing; etc.)
-  Board review

Cash Controls



Cash Disbursements

- Preparer/review of cash disbursements
- ACH/Wires – initiator and approver
- Initiator/reviewer of new vendors



Bank Reconciliation

- Prepared and reviewed timely
- Review of bank statement; access is not limited to one person

One person should not have control over the entire cash function.



Payroll, Manual Journal Entries, and Cyber



Payroll

- Access restricted to appropriate personnel
 - Employees that approve wage changes can't make the changes in the payroll cycles
- Change Log is reviewed
- Budget vs. Actual review



Manual Journal Entries

- Timely review of monthly financials
- Review non-routine journal entries
- Budget vs. Actual review



Cyber

- Phishing
- Spoofing



Cash

- Treasurer or audit committee chair should have view-only online banking access
- Dual signatures for large disbursements



Review and Oversight

- Meet at least quarterly
- Review budget-to-actual variances
- Executive sessions with external auditors



Other

- Require periodic time off for finance leadership
- Understand and scrutinize the business purpose for related party transactions
- Implement an anonymous whistleblower hotline
- Trust...but verify!



Risk & Insurance | Employee Benefits | Retirement & Private Wealth

Nonprofit Risk Management Essentials

Six Critical Areas Every Leader Should Know

Haskell and White Annual Nonprofit Conference

Agenda

What We'll Cover Today

- 1 Executive Liability (D&O)**
What coverage actually protects your leadership
- 2 Board Engagement**
Using insurance to recruit better board members
- 3 Coverage Pitfalls**
Where most nonprofit policies fall short
- 4 Abuse & Molestation Crisis**
The market reality and what you can do
- 5 AI Governance**
Your staff is already using AI. Here's what to do about it
- 6 Enterprise Risk Management**
Moving beyond the compliance checklist



Polling Question #3

Orange and blue are the colors of which NFL team?

- A. Chicago Bears
- B. Miami Dolphins
- C. Denver Broncos
- D. New York Giants

Executive Liability (D&O)

What your policy should actually cover

Side A Coverage

The Individual Protection Layer

- Protects directors and officers when the organization can't indemnify them in bankruptcy, insolvency, or regulatory actions
- Additional Defense Limits, not impacting the liability limits are available and valuable (you SHOULD have these)
- Additional Side A limits should be considered

Side B Coverage

The Organization Reimbursement Layer

- Reimburses the nonprofit when it indemnifies leaders
- Important, but secondary to Side A
- Protects organizational assets when you stand behind your team

Employment Practices Liability

The Workplace Claims Layer

- Often bundled but may have separate or shared limits
- Covers discrimination, harassment, wrongful termination claims
- Check if limits still match your current workforce size

Monday morning action: Pull out your declarations page and check your Side A limits and Additional Defense limits

Board Engagement

Using insurance as a recruitment tool

Here's something most nonprofits don't think about: your insurance coverage is part of your board recruitment pitch.

Why They Care

- Personal asset protection is non-negotiable for sophisticated board candidates
- They're comparing you to for-profit boards with robust D&O coverage
- Insurance gaps can quietly kill your ability to recruit top talent
- The question isn't if they'll ask. It's whether you'll have a good answer

What Makes a Difference

- Bring up insurance proactively in recruitment conversations
- Have a clear, confident answer about your D&O coverage
- Make sure your bylaws have strong indemnification language
- Ask candidates what insurance questions they have. Their response tells you a lot

Try this: Next board candidate interview, ask them what insurance questions they have. If they have none, you've found a coaching opportunity.

Coverage Pitfalls

Four gaps we see constantly

Your policy was written for last year's organization. Let's talk about where things have changed:

Cyber Exclusions

Your general liability policy probably excludes cyber now

You need standalone cyber coverage: ransomware, business interruption, and notification costs add up fast

Volunteer Coverage Limits

Staff are covered, but volunteers may be capped at minimal amounts

If you have hundreds of volunteers and a serious incident, those caps won't go far

International Operations

U.S. policies often stop at the border

Overseas programs and foreign national employees may not be covered under standard policies

Contractual Liability

You signed a hold-harmless clause requiring more coverage than you have

Venue contracts often require \$5M in coverage while your policy caps contractual liability at \$1M

Don't wait until renewal: Schedule a policy review now and map coverage against current operations

Abuse & Molestation Coverage Crisis

Here's what you can control

If you work with youth, this conversation isn't optional. The insurance market for abuse and molestation coverage is in crisis, and it's getting worse.

The Market Reality

- Carriers are restricting or exiting this coverage entirely
- Premium increases of 200-400% are common for youth-serving organizations
- Some insurers won't write new policies regardless of your risk controls

What You Can Control

Document Everything

Background checks, reference verification, training completion—create an audit trail that shows insurers you're serious

Clear Reporting Protocols

Staff and volunteers need to know exactly how to report concerns, and you need a documented response plan

Explore Alternatives

Risk retention groups and captive insurance aren't cheaper, but they provide stability when traditional markets won't write coverage

Start now. Not at renewal. Organizations waiting until renewal are finding themselves uninsurable.

AI Governance

Your team is already using it. Let's get practical

Let's be honest: your staff is already using ChatGPT, Claude, and other AI tools. The question isn't whether to allow it—it's how to manage it.

You don't need a 50-page policy. You need four basic guardrails:

Data Protection	Never input donor info, financial data, or PII into public AI tools One staff member feeding donor data into ChatGPT to draft thank-you letters = massive breach
Output Verification	Treat AI content as a first draft and always fact-check AI is confident but not always correct—verify accuracy and tone before anything goes out
Transparency	Disclose AI use in external communications where material Grant applications and published research may require disclosure per funder/academic standards
Access Control	Designate approved tools and create use guidelines Not all AI tools are equal from a security standpoint—choose carefully

A one-page acceptable use policy beats six months of committee debates. Get something in place and iterate.

Enterprise Risk Management

Beyond the compliance checklist

Most nonprofits approach risk as a compliance exercise. What if it could actually help you achieve your mission?

Compliance-Based

How most organizations operate:

- Checklist mentality: Are we covered on paper?
- Reactive to requirements: We do it because we have to
- Siloed risk ownership: Insurance is CFO's problem, programs are COO's
- Annual review cycle: Once a year whether we need it or not
- Risk avoidance focus: Don't do anything that creates liability

Strategic Framework

What high-impact organization do:

- Integrated across operations: Risk built into program design
- Forward-looking scenarios: What emerging risks could impact our mission?
- Shared risk ownership: Everyone owns risk in their domain
- Ongoing monitoring: Risks change, so does our assessment
- Calculated risk-taking: Sometimes mission requires accepting risk

The organizations achieving the most impact? They're the ones willing to take calculated risks for their mission.

Six Things to Do Monday Morning

- 1 Pull your D&O declarations page. Check Side A limits, Check for Additional Defense Limits
- 2 Add insurance to your next board recruitment conversation. Bring it up proactively.
- 3 Schedule a policy review before renewal and map coverage against current operations.
- 4 If you serve youth: document risk controls now and explore alternative insurance structures.
- 5 Draft a one-page AI acceptable use policy. Your staff is already using these tools
- 6 Add strategic risk discussion to next board agenda. Not just during insurance renewals.

Questions?

Thanks for being here. Let's protect your missions together.



Navigating Common Nonprofit Accounting Challenges



Frequently cited NPO “pain points”

**Contribution
accounting**

**Financial assets
and liquidity**

**Functional
expenses**

**Audit
Preparedness**



Contributions - Definition

Excerpt from ASC Master Glossary

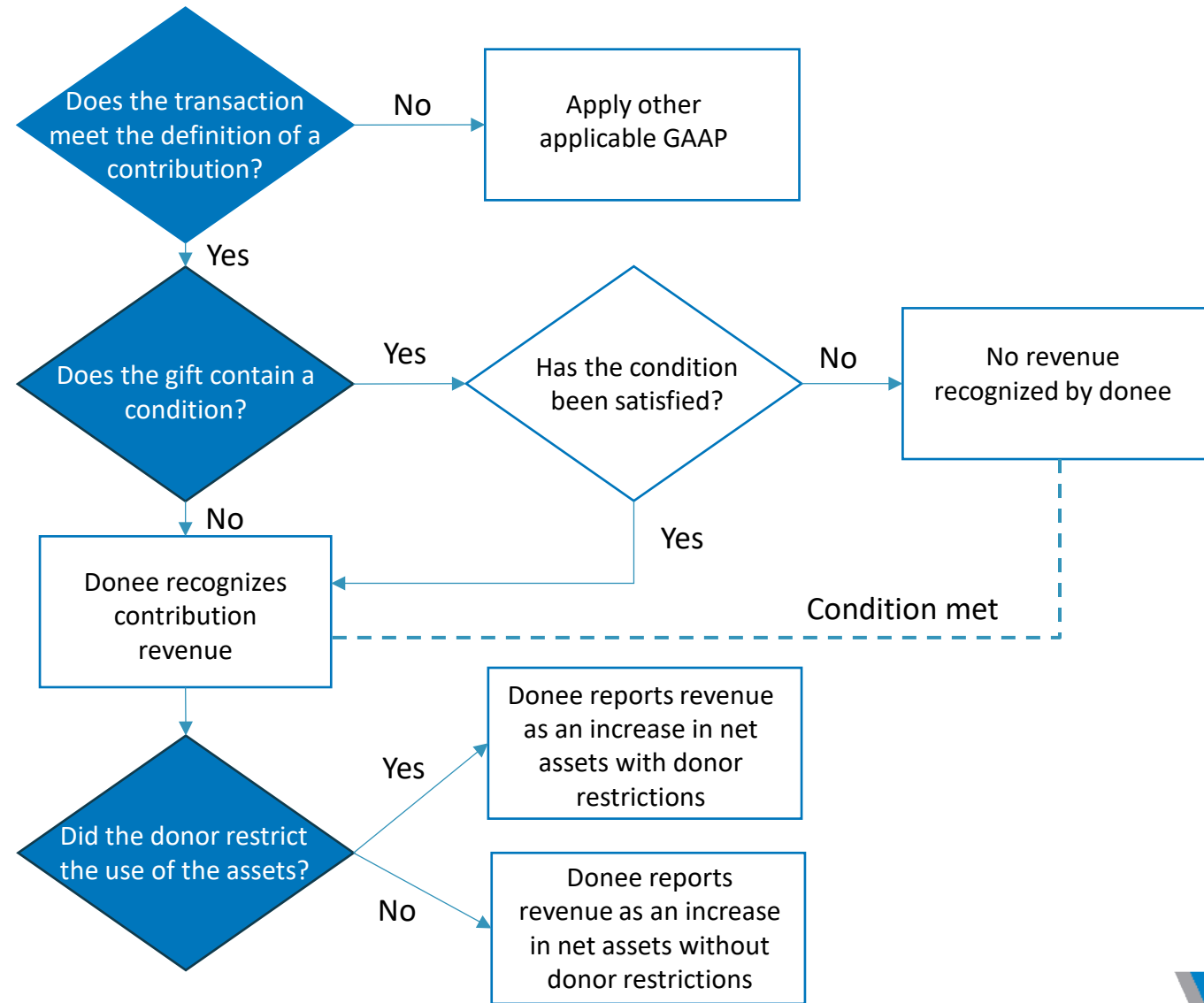
Contribution

An unconditional transfer of cash or other assets, as well as unconditional promises to give, to an entity or a reduction, settlement or cancellation of its liabilities in a voluntary **nonreciprocal transfer** by another entity acting other than as an owner. Those characteristics distinguish contributions from **exchange transactions**, which are reciprocal transfers in which each party receives and sacrifices approximately commensurate value...

In a contribution transaction, the resource provider often receives value indirectly by providing a societal benefit although that benefit is not considered to be of commensurate value. In an exchange transaction, the potential public benefits are secondary to the potential direct benefits to the resource provider.



Contributions – Your 3 Step Plan





Contributions – Step 1: Non-reciprocal transaction or exchange transaction?

In an exchange transaction, both parties receive **“commensurate value”**

Benefitting the public and furthering your mission does NOT equal commensurate value (thus, more grants are now treated as contributions)

Indicators of whether transactions are exchange or nonexchange -

Exchange	Nonexchange
The intent by both parties is to exchange resources for goods and services that are of commensurate value	Recipient solicits assets from the resource provider without the intent of providing goods or services of commensurate value
Both parties agree on the amount of assets transferred in exchange for goods and services that are of commensurate value	Resource provider has full discretion in determining the amount of the transferred assets
Contractual provisions provide for assessment of penalties beyond the amount of assets transferred if the NPO fails to perform	Penalties assessed for failure to comply with the terms of the agreement are limited to the delivery of assets/services already provided and the return of unspent funds

Source: PwC Viewpoint

Contributions – Step 2: Unconditional or Conditional?

Excerpt from [ASC 958-605-25-11](#)

Conditional promises to give, which contain donor-imposed conditions that represent a **barrier** that must be overcome as well as a **right of release from obligation**, shall be recognized when the condition or conditions on which they depend are substantially met...





Contributions – Step 2: Barriers

ASC 958-605-25-5D provides indicators to help evaluate whether stipulations included in gift and grant agreements would be considered substantive barriers:

1 Measurable performance levels or goals; specified outputs, outcomes, or levels of service

2 A specific external event must occur

3 The recipient is required to perform the activity in a specific manner (and thus, limits its discretion)

4 Reporting or administrative requirements that are directly related to achieving the grant or gift's purpose (rather than compliance-oriented)

Contributions – Step 2: Right of return/release

The right of return or release must be determinable from the gift or grant agreement. The specific phrase “right of return” or “release from obligation” does not have to appear in the agreement; however, the right (or release) should be stated sufficiently clearly to be able to support a reasonable conclusion.





Contributions – Examples related to conditions

EXAMPLE

1

The Challenge
Grant

EXAMPLE

2

Shelter Grant
requires providing
10,000 meals by
year-end

EXAMPLE

3

The “Satisfactory
Progress”
Provision

EXAMPLE

4

Provision of an
Annual
Report/Impact
Report

EXAMPLE

5

Cost-
Reimbursement
Grants



Contributions – Step 3: Evaluating Restrictions

Financial statements hinge on proper classification:

- Net assets **with donor restrictions vs. without donor restrictions.**

Misclassification impacts:

Board decisions

Liquidity perception

Grant compliance

Audit risk and findings

Common reality:

Restrictions are **not clearly communicated to accounting**

Development, legal, and accounting operate in silos

This is not solely an accounting issue.

A decorative vertical strip on the left side of the slide features a blue background with several speech bubbles of different colors (red, pink, white, yellow) containing a question mark. The bubbles are arranged in a staggered pattern.

Polling Question #4

The donations our organization receives normally has restrictions.

- A. Strongly agree
- B. Agree
- C. Disagree
- D. Strongly disagree



Contributions – Authoritative Framework (ASC 958 Overview)

Governing guidance: ASC 958-605 (Revenue Recognition for NFPs)

Core principle:

- Contributions are recognized when **received or promised**

Classification depends on:

- Presence (or absence) of **donor-imposed restrictions**

Types of restrictions:



Time Restrictions



Purpose Restrictions



Perpetual Restrictions
(Endowments)

Remember — Board designations are not restrictions!



Contributions with Restrictions - Real World Challenges

1 Incomplete documentation

- Agreements not standardized
- Missing amendments or side letters
- Lack of formalized system; spreadsheet tracking vs. software

2 Development vs. accounting disconnect

- Development teams interpret donor intent differently
- Accounting receives summaries, not source documents

3 Ambiguous donor language

- Terms like “support,” “help,” “advance” lack clarity

4 Timing issues

- Restrictions expire over time, but releases are not tracked

5 Multi-year grants



Contributions with Restrictions - What can we do?



Cross-department communication

Accountants - go have lunch with the development people!



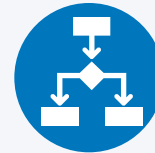
Standardized forms and language

No 'one-offs'



Process design and controls

Utilize software and maintain centralized storage. If I have a question, who do I ask?



Decision tree / flow chart

Contemporaneous determination

Is there a donor restriction? Yes, no? If yes, what kind?

Accountant

"What does this mean in the donation letter?"

Development Director

"I don't know, but I don't want to go back to the donor and ask as it might upset them."



Contributions with Restrictions - Key Takeaways

1

Restrictions impact operational flexibility. So we need to know them.

2

Improper classification or use can mislead stakeholders

3

Have consistency in documentation

4

Build/improve processes and controls

5

Cross-department communication



Liquidity Disclosure in NFP

Technical requirement under ASC 958-210-50

- Nothing new, but we still see implementation challenges. There are examples in the standard.
- Has this been easy, are you satisfied with how this is working?

Quantitative Disclosures

**Financial Assets
at balance
sheet date**

Less:

**Donor restrictions
(Time / purpose)**

**Board designations
(If not available)**

**Contractual/
legal
limitations**

**Result:
Financial assets available
within 1 Year**

Liquidity Disclosure Example

Financial assets available to meet general expenditures within one year	
Financial assets at year end	Amount
Cash and cash equivalents	\$1,000
Short-term investments	\$50
Accounts receivable	\$300
Contributions receivable (net)	\$200
Other financial assets	\$50
Total financial assets	<u>\$1,600</u>
Less amounts not available within one year	
Adjustments	Amount
Donor-restricted for purpose or time	(\$250)
Endowment funds (perpetual in nature)	(\$200)
Endowment earnings not appropriated	(\$100)
Board-designated reserves	(\$50)
Financial assets not liquid or not expected to be realized within one year	(\$100)
Other contractual or legal restrictions	(\$100)
Total amounts not available	<u>(\$800)</u>
	Amount
Financial assets available to meet general expenditures within one year	<u>\$800</u>



Liquidity - Qualitative Disclosures

How the organization manages liquidity, including:

Cash flow practices

Lines of credit

Reserve policies

Timing of receivables
and payables

Example:

The Organization maintains a policy of structuring its financial assets to be available as general expenditures, liabilities, and other obligations come due. Cash flows are monitored on a regular basis to ensure that sufficient resources are available to meet operating needs.

The Organization receives significant contributions and grants, many of which are restricted for specific programs or future periods. As a result, the Organization manages liquidity by aligning the timing of cash inflows from these restricted resources with related program expenditures.

To support short-term liquidity needs, the Organization maintains operating cash reserves and may utilize a line of credit, if necessary. The Organization's goal is generally to maintain liquid assets sufficient to cover a defined period of operating expenses.

In addition, the Organization has established board-designated reserves intended to provide financial stability and support mission-related opportunities. While these amounts are not intended for general expenditure, they could be made available if necessary through board action.

Endowment funds are held for long-term purposes, with annual appropriations made in accordance with the Organization's spending policy.



Liquidity - Drafting Challenges

Restriction information is not always clear, from both donors and board designations.



What does 'available' mean?



Are all pledged contributions collectible?



Can you use earnings from the endowment?
How much?

As you can see, not strictly an accounting exercise.



Liquidity - Stakeholders Use/Interpretation

Disclosure should be realistic and 'true presentation'

Not overly optimistic but not dire emergency

Disclosure acts as a 'stress test' for the organization

Can it withstand short term liquidity challenges?

Impact on donor giving

How flexible is the organization?

Restrictions and board designations too restrictive?

Is it telling the true 'story'?



Functional Expense Allocation

The relationship between functional classification (Program Services and Supporting Activities, which are Management & General and Fundraising) and natural classification (Salaries/Occupancy/Professional) for all expenses shall be presented in an analysis that disaggregates functional expense classifications by their natural expense classifications.

Why is this important?



Important Definitions

DEFINITION

Program Services

The activities that result in goods and services being distributed to beneficiaries, customers, or members that fulfill the purposes or mission for which the not-for-profit entity exists.

DEFINITION

Supporting Activities

...all activities of a not-for-profit entity other than program services. Generally, they include management and general activities, fundraising activities, and membership development activities.



Surprise – these costs are defined as Supporting Activities



**Organizational oversight;
budgeting, finance and
management**



**General record-keeping and
payroll**



**Employee benefits
management and oversight
(human resources)**



Let's do it – Direct Identification vs. Cost Allocations

Direct

If an expense can be specifically identified with a program or supporting service, it should be assigned to that function. For example, travel costs incurred in connection with a program activity would be assigned to that program.

Cost Allocations

When direct identification is impossible or impracticable, an allocation is appropriate.

- Rational, systematic, and reasonable
- Applied consistently (unless facts and circumstances change)
- Objective methods > subjective methods
- No “one-size-fits-all” model



Polling Question #5

ChatGPT knows the exact amount of time my CEO spent on program services, fundraising, and managing the organization last year.

- A. True
- B. False



Sample Note Disclosure (from ASC 958-205)

SAMPLE NOTE DISCLOSURE

The financial statements report certain categories of expenses that are attributable to more than one program or supporting function. Therefore, these expenses require allocation on a reasonable basis that is consistently applied. The expenses that are allocated include depreciation, interest, and office and occupancy, which are allocated on a square-footage basis, as well as salaries and benefits, which are allocated on the basis of estimates of time and effort.



Is there a “magic percentage”? Simple answer – no!

2013 — JOINT STATEMENT

GuideStar, Charity Navigator & BBB

Jointly warned against over-reliance on overhead ratios, coining what's often called the "overhead myth."

However, other agencies and donors may still look at the ratio and believe that, **as a general rule, this ratio should not exceed 35%.**

Many leading organizations have recognized the real need to invest in supporting services and have responded by altering the ways they measure performance across NFPs.



Holistic Approach

STRATEGY -

Educate stakeholders on a more holistic approach to nonprofit evaluation.

1

Transparency

2

Governance

3

Measurable
outcomes

4

Financial
sustainability

5

Strategic
investment

Audit Preparedness





Audit Preparedness



Be prepared

- Keep up accounting for transactions year-round
- Don't wait until after year-end to figure out new or difficult items
- Call your accountants, we like to talk to you!



Sufficient resources

- Be realistic about the hours in the day and putting the audit work on top of the accounting team's day job
- Have buy-in with all stakeholders. Is the Executive Director promising timelines that are not achievable? Silent acquiescence by lower-level staff. Board members can help here.



Use the checklist

- Review the checklist we provided last year and take notes!

Right-Sized Security: Practical Cybersecurity for Nonprofits





Polling Question #6

How many suspicious or phishing emails do you personally receive per week?

- A. 0 to 2
- B. 3 to 5
- C. 6 to 10
- D. 11 to 15
- E. 15+
- F. Not sure / I don't track

ONE CLICK: \$60,000 GONE

A single phishing email. No sophisticated hacker. No advanced technology.



The attack did not require a sophisticated hacker or advanced technology.



Only one click and one missing control that costs nothing to implement.



The organization looked like many non-profits: outsourced IT, no internal security team, no CISO



Good News: The controls that would have stopped it are available to every organization in this room



THE REAL THREATS

NOBODY is too small to be targeted.

Nonprofits are increasingly in the crosshairs

Most don't have the resources for a full-time IT security leader (which attackers know)

Three Most Common Attacks Impacting Nonprofits:



Business Email Compromise (BEC)

Attacker compromises or impersonates
a legitimate email



Ransomware

Attacker encrypts your data, demands
payment to restore



Credential Theft via Phishing

Someone clicks a link, enters their
Microsoft 365 or Google Workspace
password into a fake page, and the
attack "owns" that account

The common thread: All three attacks succeed most often when just one or two basic security controls are missing in an organization.



Five High-Impact, Low-Friction Controls

The five highest impact, lowest friction security controls that most organizations miss (and most of them are free):

1

Multi-Factor Authentication (MFA)

2

Use a Password Manager

3

The 3-2-1 Rule For Backups

4

Secure Email with DNS Records (SPF, DKIM, DMARC)

5

Cyber Insurance – And Understanding What It Requires



Control #1: MULTI-FACTOR AUTHENTICATION (MFA)

- A second layer of verification at login — typically a push notification or a code sent to your phone
- Even if an attacker steals your password, they cannot access your account without the second factor
- Microsoft has reported that MFA blocks over 99% of automated credential attacks
- Included at no additional cost in Microsoft 365 and Google Workspace — it requires configuration, not purchase
- The most common miss: MFA is available but not turned on for everyone — part-time staff, contractors, and board members with organizational email are frequently missed!
- Don't forget your financial accounts and web facing business critical applications!

MFA is not just for email — enable it everywhere:

- Online banking and financial accounts
- Donor management and CRM platforms
- Payroll and HR systems
- Any web-facing application your organization depends on



ASK YOUR IT VENDOR TODAY

"Is MFA enabled on every single email account in our organization — no exceptions?"



Control #2: USE PASSWORD MANAGERS

- Password reuse is one of the most common and preventable causes of account compromise
- If an employee reuses a password from a breached website, attackers do not need to hack you — they just log in
- A password manager generates and stores unique, complex passwords for every account
- Staff are not reusing passwords because they are careless — they are doing it because remembering dozens of passwords without a tool is genuinely impossible

What it costs:

- Bitwarden — free for individuals, approximately \$3/user/month for teams
- 1Password and LastPass both offer nonprofit pricing
- For a 20-person organization, expect roughly \$60/month or less



ASK YOUR IT VENDOR TODAY

“Do we have a password manager deployed for our staff?”



Control #3: The 3-2-1 RULE OF BACKUPS

The

3-2-1

Rule

3

Copies of your data (original + two copies)

2

Different storage types (e.g., local external hard drive & cloud storage)

1

Copy offsite or cloud-based (disconnected from your systems)



THREE QUESTIONS TO ASK YOUR IT VENDOR TODAY

1. **Where are our backups stored — and are any of them offline or disconnected from our network?**
2. **When did we last actually test a restore — not just confirm the backup ran, but pull a file back and confirm it worked?**
3. **If we got hit with ransomware tomorrow, how long would recovery take and what would we lose?**



Control #4: SECURE YOUR EMAIL (SPF, DKIM, DMARC)

Attackers routinely send emails that appear to come from your organization in an attempt to impersonate your employees or vendors.

Three email authentication standards exist specifically to mitigate this – most organizations are not aware they exist!

SPF (Sender Policy Framework) – Specifies which mail servers are authorized to send email on behalf of your domain (e.g., “@ournonprofit.org”)

DKIM (DomainKeys Identified Mail) – Cryptographically signs outgoing emails that receiving servers use to verify authenticity

DMARC (Domain-based Message Authentication, Reporting and Conformance) – Ties SPF and DKIM together and tells receiving mail servers what to do with emails that fail authentication. Sends you reports when someone tries to spoof your domain

? ASK YOUR IT VENDOR TODAY

"Do we have SPF, DKIM, and DMARC configured on our email domain — and is DMARC set to reject or quarantine failing messages?"



Control #5: CYBER INSURANCE – AND UNDERSTANDING WHAT IT REQUIRES

Cyber insurance is your financial safety net when the first four controls get tested

A standalone cyber policy for a small nonprofit is often available for \$1,500 — \$3,500 per year

Coverage typically includes: BEC and wire fraud losses, ransomware response costs, breach notification expenses, regulatory defense, and crisis communications

What insurers now require — and will deny claims without:

- MFA on email and remote access
- Tested backups
- Endpoint protection (antivirus/EDR) on all devices
- Documented incident response plan
- Security awareness training



THREE QUESTIONS TO ASK ABOUT YOUR CURRENT POLICY:

- Do we have a standalone cyber policy — or are we relying on a rider on our general liability?
- When did we last review our coverage conditions against our actual security controls?
- Does our policy cover funds transfer fraud and social engineering losses?



Polling Question #7

How confident are you that MFA is enabled on every email account in your organization — including part-time staff, contractors, and board members?

- A. Very confident — we have verified this
- B. Somewhat confident — but we have not formally verified
- C. We have it for some staff, but not all
- D. We do not have MFA in place
- E. I am not sure

SECURITY GOVERNANCE WITHOUT BUREAUCRACY

You may not need a full-time CISO. But you do need *someone* to own cybersecurity.

At a minimum, every organization needs:

1. An owner at the leadership level whose job is to ask the right questions
2. Three honest conversations a year with your IT vendor
3. A one-page incident response plan — not a document in a drawer nobody reads
4. An annual cyber insurance review — treat it like your other insurance policies

A Common Gap With Outsourced IT:

- Your IT vendor is primarily focused on keeping your systems running — they are not typically strategic advisors or security auditors
- Non-technical leaders often don't know the right questions to ask or have no way to know whether the answers they are getting are complete, accurate or in their organization's best interest

The fractional vCISO option:

- Senior security leadership without a full-time hire
- Typically, 4 to 8 hours per month
- Right-sized for organizations with no internal IT expertise and those who have outgrown their reliance on their IT vendor for security steering.

TAKE ONE ACTION TODAY

Everything we covered today matters — but don't try to do all of it at once.

START WITH JUST ONE QUESTION

"Is multi-factor authentication turned on for every single person who has an email account with our organization — no exceptions?"

IF YES

Great! Ask them to confirm that in writing.

IF NO

This just became your most important technology conversation of the year!

RESOURCES

CISA Free Tools and Services

cisa.gov/resources-tools

MS-ISAC Free Nonprofit Membership

cisecurity.org/ms-isac

Password Managers

Bitwarden, LastPass,
1Password

FBI Internet Crime Complaint Center

ic3.gov

Nonprofit Conference

Q&A and Thank You



HASKELLWHITE

CERTIFIED PUBLIC ACCOUNTANTS | BUSINESS ADVISORS

THE VALUE OF
EXPERIENCE



Event Evaluation

Please fill out the paper form on your table or use this link

<https://www.surveymonkey.com/r/38KC2XS>

or the QR Code to access an electronic copy

