Bridging the gaps

Financial reporting deficiencies, IT control findings, and SAS No. 145

July 23, 2026

SIKICH®

Meet your speakers

Anthony Cervini, CPA, CFE

Principal

anthony.cervini@sikich.com

Amy Sherwood, CPA, CISA

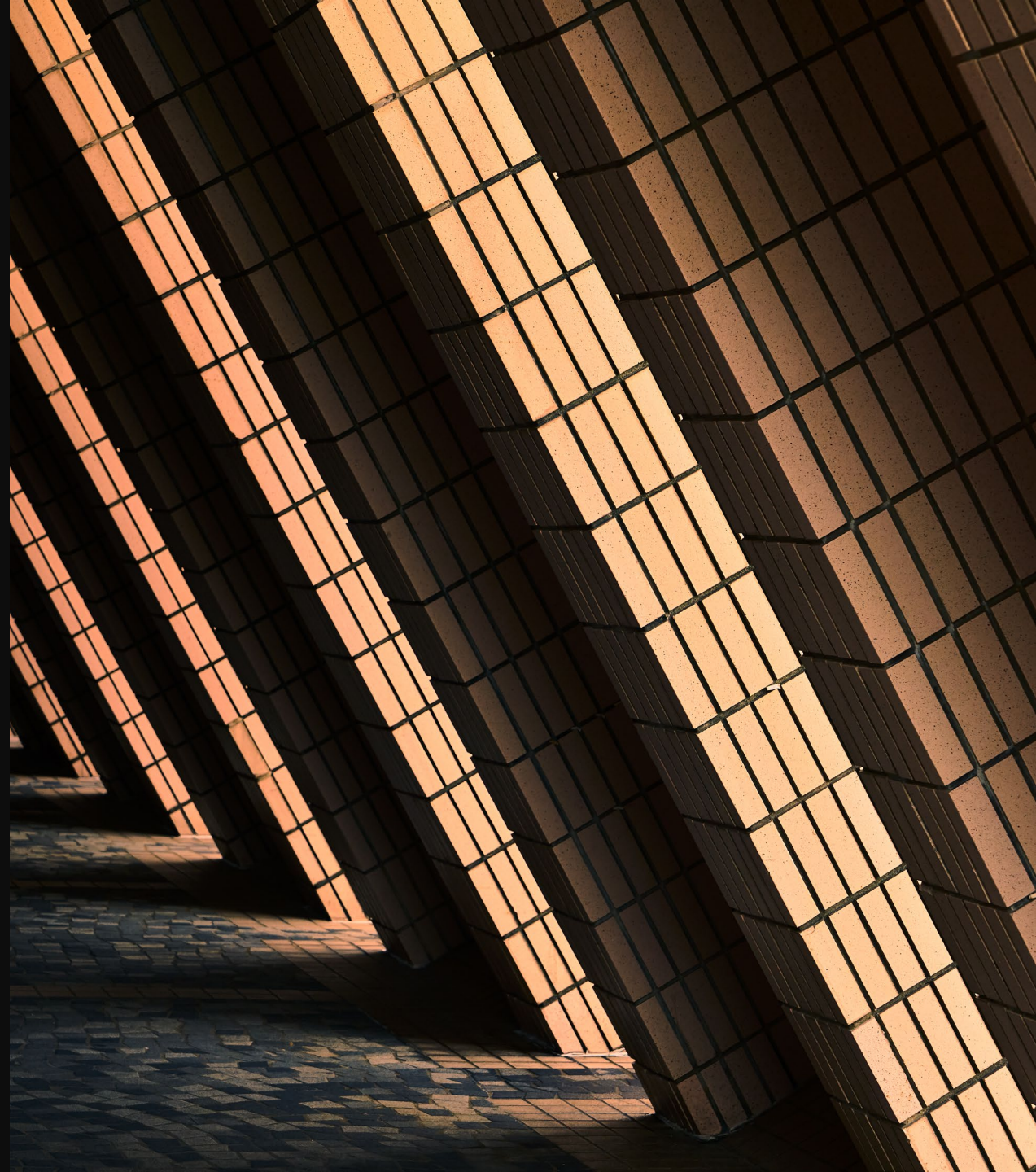
Principal

amy.sherwood@sikich.com

Table of contents

- Common financial reporting deficiencies
- IT control findings
- SAS no. 145 overview and application
- Q&A

Common financial reporting deficiencies



GASB Statement No. 101

Common errors

- Improper assumption on sick time usage
- Salary-related payments
- Improper estimate – multiple union contracts
- Missing disclosures

GASB 101 Improper assumptions

Issue	Root cause	Relevant guidance
Assume 50% of accrued unused sick time is paid out in cash at termination/retirement. Assume that 5% of unused sick time is typically converted into defined benefit pension service time credit when an employee retires. Calculation of accrued sick time assumes all to be used or paid out so therefore all should be accrued.	Inadequate understanding of settlement. Inadequate knowledge of settlement trends.	Paragraph 9 – liability recognized for leave that is attributable to services already rendered, accumulates, and is more likely than not to be used for time off or otherwise paid in cash or settled through noncash means. Paragraph 13 – settlement through conversion to defined benefit postemployment benefits is not recognized.

GASB 101 Improper assumptions

Suggested corrective actions

- Obtain historical usage reports for a selected period of time
  - 3 years, 5 years, 7 years, etc.
  - May need to break down by department due to different classes of employees.
- Obtain historical conversion reports for a selected period of time
  - Use the same breakdown as usage reports.
- Determine accrued sick time settled via anticipated usage
  - Could be % of time used divided by time earned in a single period or time accumulated to date.
  - No set required approach per Statement 101.
- Determine accrued sick time converted to defined benefit pension plan service credit

GASB 101 – Improper assumptions (cont.)

Suggested corrective actions

- Calculate liability amount assuming hours × rate of pay at reporting date.
- Total accrued unused sick time × anticipated cash %
- Plus, total accrued unused sick time × anticipated usage %
- Total compensated absence liability for sick time
  - Since this formula focuses only on the amounts to be included, conversion to DB benefits is naturally excluded.
  - If the calculation starts with total accrued unused sick time and backs out amounts that will not be settled or converted, the conversion should appear in the formula.

REMINDER:

Established procedures should be revised to reflect the correct approach and communicated to all stakeholders.

GASB 101—Salary-related payments

Issue	Root cause	Relevant guidance
Missing salary-related payments in the compensated absence liability, such as Medicare and Social Security.	Past inaccurate calculations when applying GASB Statement No. 16.	Paragraph 23 – salary-related payments that are directly and incrementally associated with the leave, not including payments for defined benefit postemployment benefits, should be included in the liability.

GASB 101—Salary-related payments

Suggested corrective actions

- Identify the salary-related payment population that is direct and incremental to the benefit
  - Medicare and Social Security are common and typically calculated as a percentage of the rate of pay.
- Ensure that defined benefit postemployment payments are not included in the payment population
- Calculate additional liability amount assuming hours × rate of pay at reporting date
- Pay rate liability previously calculated × salary-related payment %
  - Update and communicate changes to the procedures to make sure the issue does not recur.

GASB 101 Improper estimates

Union contracts

Issue	Root cause	Relevant guidance
Using a singular approach across all entity departments to estimate the compensated absence liability when clear department-level differences exist regarding amounts earned and used.	Inadequate understanding of the types of benefits offered versus the various classes of department employees.	Paragraph 12 – leave settlement should be evaluated using relevant factors, including existing policies, future use or payment expectations, historical use/payment/forfeiture, and information indicating historical data may not represent future trends.

GASB 101 Improper estimates

Union contracts– suggested corrective actions

- Determine the complete population of benefit types offered and the degree of benefit diversification among employees
- Maintain an inventory of applicable policies and union contracts.
- Coordination with departments regarding changes is critical
- Perform annual update of populations of benefits available
- Update the library of union contracts and employee policies.
- Reflect updated contract and policy information in year-end compensated absence liability calculations.

REMINDER:

Ensure benefit population updates are reflected in the procedures used to calculate the compensated absence liability.

GASB 101 Missing disclosures

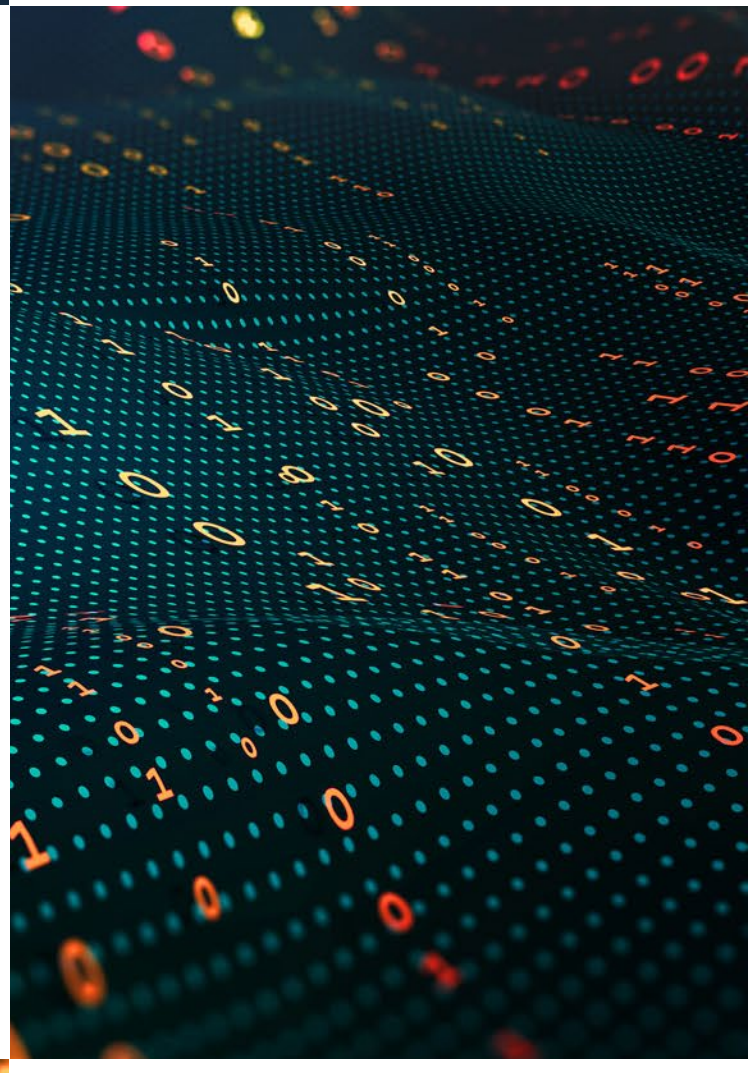
Issue	Root cause	Relevant guidance
Missing disclosure in the long-term debt roll forward footnote that a net increase/decrease was used.	Missed new requirement in GASB Statement No. 101 during adoption.	Paragraph 30 – notes should present either separate increases/decreases or a net increase/decrease with a separate indicator that the rollforward amount is a net amount.

GASB 101 – Missing disclosures (cont.)

Suggested corrective actions

- Review the footnote disclosure from the prior year to determine what approach was used.
- Revise the footnote disclosure appropriately, including the additional disclosure that the additions/deletions in the roll forward note are a net amount.

Polling question #1



SIKICH

GASB Statement No. 87/96

Common errors

- **Contract modifications**
- Agreement changes for lease term and payments
- Determination of reasonably certain extensions that will be exercised/terminated
- **Incorrect assessment of initial terms for cancellable/noncancellable portions of the agreement**

*For GASB 87, focus will be on the lessee side and the liabilities, not the ROU assets.

GASB 87/96 – agreement changes

Issue	Root cause	Relevant guidance
Agreement is modified and impacts the term of the lease and payment structure, but the entity continues to account for the lease/SBITA under the original agreement language. Assume the modification does not provide an additional asset that would be a separate lease/SBITA.	Inadequate monitoring of contracts.	GASB 87 paragraph 73 – amendment would be accounted for as a modification requiring remeasurement of the lease liability, with potential discount rate update per paragraph 27. GASB 96 paragraph 55 – similar language.

GASB 87/96– agreement changes

Suggested corrective actions

- Identify the point in time where the agreement modification took place
- Remeasure the lease/SBITA liability as of the modification date
- If the modification occurred in a prior reporting period, determine whether the corresponding impact is an immaterial adjustment or requires restatement.
- Do not forget to update the discount rate.
- Update lease/SBITA accounting policies and procedures to include monitoring of existing agreements for modifications

GASB 87/96 – extension determinations

Issue	Root cause	Relevant guidance
Before expiration of a lease in a subsequent reporting period, an extension initially determined to be reasonably certain to be exercised now has factors that indicate the extension will not be exercised, but accounting is not updated. The agreement was not terminated.	Inadequate monitoring of contracts.	GASB 87 paragraph 12 – lease term includes periods covered by lessee option to extend if reasonably certain to be exercised, or option to terminate if reasonably certain not to be exercised. GASB 87 paragraph 15 – reassess lease term if an option to extend previously considered reasonably certain is not exercised. GASB 96 paragraphs 9 and 12 – similar language

GASB 87/96– extension determinations

Suggested corrective actions

- Identify the point in time where the extension determination changed
- Use the extension exercise date per the agreement if it occurred before agreement termination.
- Remeasure the lease liability using the modified lease term
- Update lease/SBITA accounting policies and procedures to include monitoring of existing agreements for modifications.

Reminder:

Updated procedures so changed extension decisions are captured before financial reporting close.

GASB 87/96 – Incorrect initial assessment of term

Issue	Root cause	Relevant guidance
Lease term is initially incorrectly determined due to cancellable/noncancellable portions.	Incorrect assessment of lease term because lessee/lessor termination rights are not fully understood.	GASB 87 paragraph 12 – periods in which both the lessee and lessor can terminate without permission are excluded from lease term. GASB 96 paragraph 9 – similar language.

GASB 87/96 – Incorrect initial assessment of term

Suggested corrective actions

- Re-review the agreement and fully document the ability of both parties to cancel the lease/SBITA.
- Re-compute the lease/SBITA liability with the corrected term.
- This would be considered correction of an error.
- Consider additional controls/procedures over initial calculations so error occurrence is reduced.

Reminder:

Consider controls over initial calculations to reduce recurrence.

Polling question #2

Net investment in capital assets

Suggested corrective actions

- Calculation often incorrect or incomplete due to missing information
- Deferred amount on refunding
- Accounts payable / retainage payable
- Leases / SBITAs
- Including amounts not subject to the calculation
- Accrued interest payable
- Looking for a resource? GFOA has a template available on its website.

NICA examples

Suggestive corrective actions

- Use examples to demonstrate how debt, leases, SBITAs, refunding deferrals, retainage and capital asset balances are evaluated in the net investment in capital assets calculation.
- Tie the calculation back to the government-wide statement of net position and related debt/capital asset footnotes.

Cash flows

Suggestive corrective actions

- Purchase of capital assets
- Treatment of accounts payable / retainage payable
- Default category is operating – both for cash flows and income statement.
- Both statements have different sets of definitions for non-operating.
- Non-cash items not disclosed.

RSI– Budgetary comparison schedules

Suggested corrective actions

- **Which budgetary comparison schedules are reported as RSI?**
- General Fund
- Major special revenue funds
- Nonmajor special revenue funds (not RSI)
- Debt service funds (not RSI)
- Capital project funds (not RSI)
- Permanent funds (not RSI)

Other items

Suggested corrective actions

- Budget versus actual presentations – level of detail insufficient to show legal compliance; variance column calculations.
- Non-GAAP presentations – including items as RSI under OCBOA, where there is no RSI.
- Required for all governmental funds with legally adopted, time-based budgets.

- Articulation
- Long-term liabilities / MD&A
- Debt issuances
- Debt capacity schedules – statistical section
- Net Position
- Reporting major categories
- Unspent proceeds

Major fund determination

Suggested corrective actions

- Transfers versus subsidies

GASB 103

MD&A / Presentation readiness

Issue	Root cause	Suggested corrective actions
▪ MD&A repeats amounts or percentages without explaining why changes occurred. ▪ Budgetary comparison templates are not updated for required variance presentation. ▪ Operating vs. nonoperating classifications are not re-evaluated for proprietary funds.	Prior-year language and schedules are rolled forward before financial reporting model changes are embedded in the close checklist.	▪ Rebuild MD&A around required sections and remove boilerplate language. ▪ For each significant variance, document the underlying driver, not just the dollar change. ▪ Update budgetary comparison RSI templates before close begins. ▪ Flag unusual/infrequent items and proprietary fund classifications for controller-level review.

Fund balance + revenue recognition

Issue	Root cause	Suggested corrective actions
▪ Restricted, committed, assigned and unassigned balances are not supported by the underlying constraint or formal action. ▪ Grant, tax or other nonexchange revenue is recognized before eligibility, time requirements or availability are met. ▪ Unavailable revenue and unearned revenue are used interchangeably.	Constraint approvals, grant terms and the entity's availability policy are not tied into a single year-end revenue review.	▪ Maintain a fund balance worksheet by funding source, constraint and approval authority. ▪ Retain formal support for committed and assigned fund balance decisions. ▪ Tie each receivable and deferred inflow to eligibility, time requirements and the availability window. ▪ Add a close review for advance receipts versus earned but unavailable resources.

Disclosure schedules

Tie-out risks

Issue	Root cause	Relevant guidance	Suggested corrective actions
▪ Cash and investment risk disclosures do not agree to the portfolio, collateral records or investment policy. ▪ Pension/OPEB entries, deferrals and RSI schedules do not agree to actuarial or plan reports. ▪ Footnotes are rolled forward without refreshing dates, assumptions and contribution data.	Disclosure owners receive support late and there is no independent tie-out from the note to the source document.	GASB 40 deposits/investments; GASB 68 pensions; GASB 75 OPEB	▪ Build a disclosure binder with source support for each note and RSI schedule. ▪ Tie risk disclosures to bank confirmations, investment statements and written policies. ▪ Reconcile GASB 68/75 entries to actuarial reports, including deferrals and subsequent contributions. ▪ Update RSI and footnotes for the correct measurement and valuation dates.

Completeness checks

Assets + reporting entity

Issue	Root cause	Suggested corrective actions
▪ Capital asset rollforwards omit disposals, retainage, lease/SBITA assets or intangible assets. ▪ Component unit conclusions are not refreshed after governance, funding or operational changes. ▪ Debt/refunding disclosures omit deferred amounts, defeasance or pledged-asset impacts.	▪ Information from operations, legal and debt management is not synchronized with the finance close calendar.	▪ Use annual asset inventory and disposal certifications; reconcile additions to AP and project records. ▪ Track lease, SBITA, intangible and held-for-sale assets separately by major class. ▪ Send an annual component unit questionnaire and document blending or discrete-presentation conclusions. ▪ Review debt support for deferred amounts, defeasance, escrow and collateral disclosure requirements.

Most common audit adjustments we continue to see

Prioritize issues that create repeat findings, late adjustments or footnote rework.

1	**Pension/OPEB**	Deferrals, subsequent contributions and RSI schedules do not agree to actuarial reports.
2	**Grant revenue**	Eligibility, time requirements and availability are not evaluated consistently.
3	**Capital assets/CIP**	Completed projects remain in CIP; disposals and depreciation are missed.
4	**Debt/refunding**	Premiums, discounts, defeasance and debt service tables do not tie out.
5	**Close documentation**	Subsequent events, new contracts and legal matters are not formally captured before issuance.

Pension and OPEB deferral errors

Issue	Root cause	Suggested corrective actions
▪ Deferred outflows/inflows are recorded in the wrong year or wrong category. ▪ Subsequent contributions are omitted or do not agree to payroll/contribution support. ▪ RSI schedules use stale measurement dates, assumptions or covered payroll information.	Prior-year journal entries are used as the starting point without a full actuarial tie-out. Finance, payroll and plan administrator support arrives late and entries/notes are prepared by different owners.	▪ Create a GASB 68/75 close checklist by plan. ▪ Reconcile liability, expense, deferrals and subsequent contributions to source reports. ▪ Independently tie RSI and footnote amounts to actuarial schedules before issuance. ▪ High relevance for IMRF, police pension, firefighter pension and OPEB reporting.

Grant revenue recognition and deferred inflows

Issue	Root cause	Suggested corrective actions
▪ Revenue is recognized before eligibility or time requirements are met. ▪ Advance receipts are not evaluated for unearned revenue treatment. ▪ Unavailable revenue is not recorded when modified accrual availability criteria are not met.	Grant compliance is decentralized across departments. Close procedures do not distinguish eligibility, time requirement and availability tests. Receivable, deferred inflow and unearned revenue reviews are performed separately.	▪ Maintain a grant-by-grant compliance matrix. ▪ Tie each receivable and deferred balance to the grant agreement and expenditure support. ▪ Review advance-funded grants separately from reimbursement-based grants. ▪ Audience hook: “The invoice date is not always the revenue recognition date.”

Capital asset disposal and CIP closeout

Issue	Root cause	Suggested corrective actions
▪ Completed projects remain in construction-in-progress. ▪ Disposals, trade-ins and replaced assets are not removed from the ledger. ▪ Depreciation begins late or useful lives are not updated for major improvements.	Project completion is not tied to the year-end financial reporting checklist. Disposal information is tracked outside accounting. Retainage, AP and project records are not reconciled to capital additions.	▪ Prepare a CIP aging analysis and obtain department completion certifications. ▪ Reconcile additions to AP, retainage and project management records. ▪ Perform an annual disposal and impairment review with operating departments. ▪ Best control: require finance sign-off before projects are closed in the project system.

Debt, refunding and amortization - tie outs

Issue	Root cause	Suggested corrective actions
▪ Premiums, discounts and deferred amounts on refunding are amortized incorrectly. ▪ Defeased debt, escrow balances or pledged revenues are omitted from disclosures. ▪ Debt service schedules do not agree to trustee statements or amortization tables.	Debt schedules are maintained outside the financial reporting workbook. New debt issuances and refundings are not communicated early enough. Disclosure preparers do not have final bond transcripts or trustee support.	▪ Reconcile debt by issue to bond transcripts, trustee statements and GL activity. ▪ Perform a dedicate Use a rollforward that separately tracks principal, premiums, discounts and refunding deferrals. ▪ d disclosure tie-out for defeasance and pledged revenue language. ▪ Practical reminder: debt rollforwards, NICA and statistical debt schedules should articulate.

Fund classification and close documentation gaps

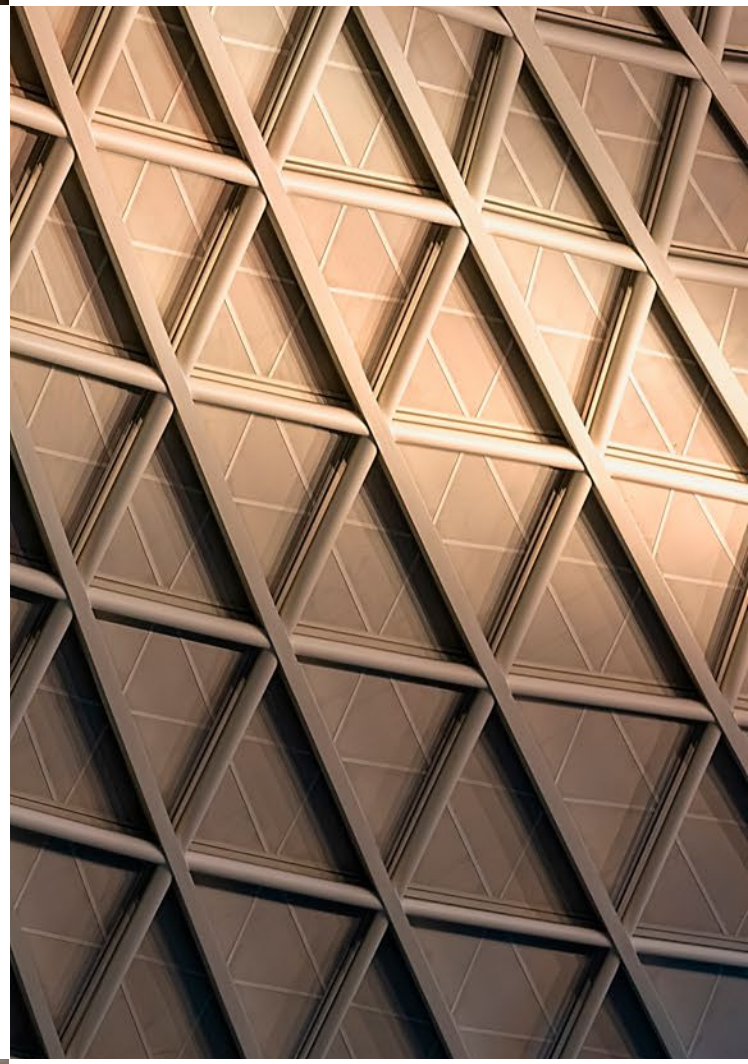
Issue	Root cause	Suggested corrective actions
▪ Internal service fund charges are not supported by allocation methodology or customer base. ▪ Enterprise fund classifications are rolled forward without re-evaluating activity and external users. ▪ Debt issuances, major contracts, litigation, grant awards and board actions before issuance are not formally evaluated.	▪ Some reporting deficiencies are not technical calculation issues; they are evidence and ownership issues. Management review may be informal or not documented.	▪ Re-evaluate fund classification and interfund activity during planning, not after draft statements. ▪ Document allocation methodology for internal service fund charges annually. ▪ Use a required subsequent events questionnaire before report issuance. ▪ Review board minutes, legal letters, debt activity and significant contracts through issuance date.

How to reduce repeat reporting deficiencies

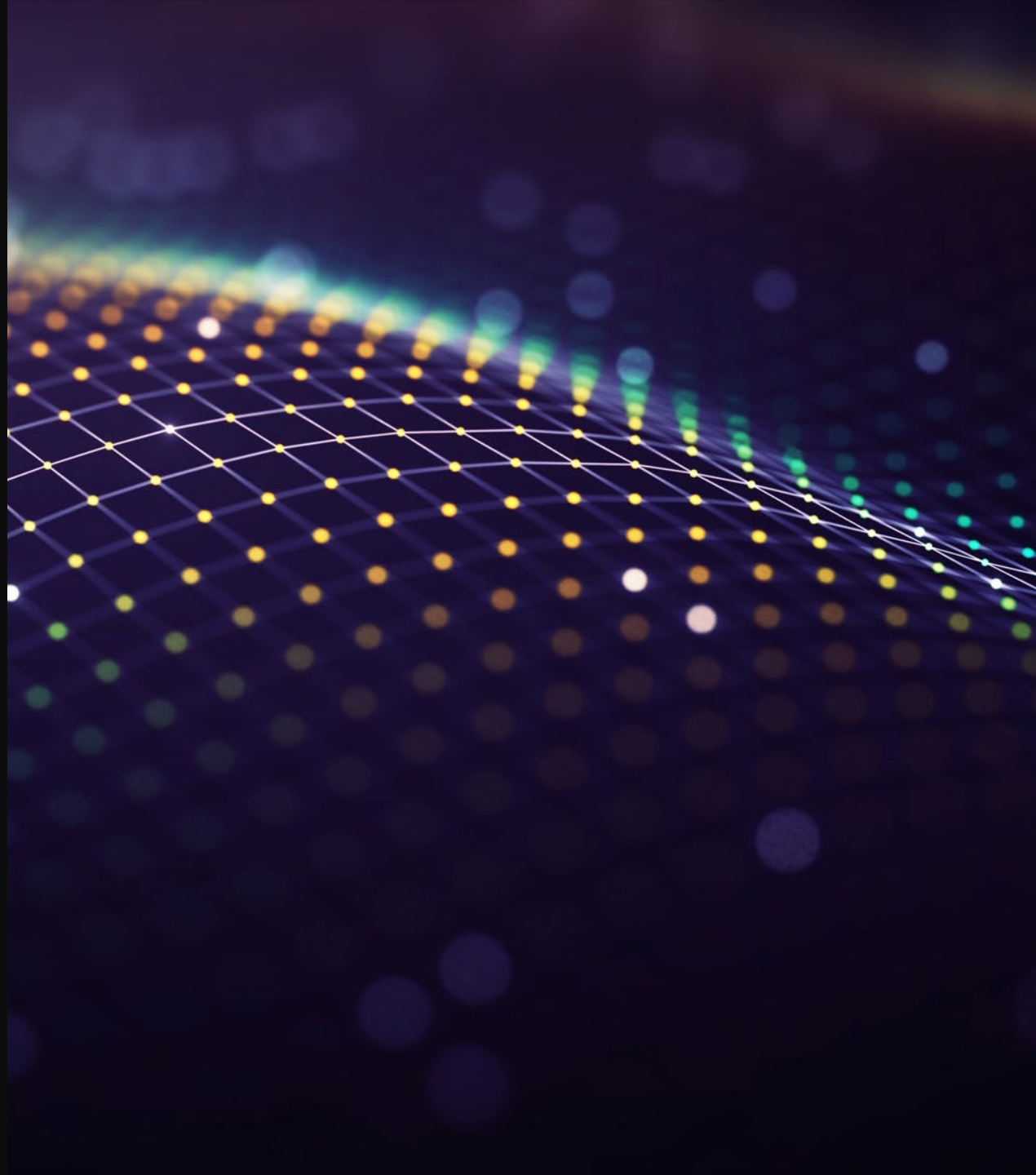
A simple close discipline can prevent many of the items discussed throughout this session.

1	**Assign ownership**	Every note, RSI schedule and estimate needs a named preparer and reviewer.
2	**Tie to source support**	Actuarial reports, grant agreements, debt schedules and capital asset records should be cross-referenced.
3	**Refresh assumptions**	Do not roll forward terms, dates, rates, classifications or variance explanations without review.
4	**Document judgment**	Reasonably certain options, availability periods, fund balance constraints and subsequent events need evidence.
5	**Perform articulation checks**	MD&A, statements, notes, RSI and statistical schedules should tell the same story.

Polling question #3



IT control findings



Why IT controls matter in government

Directly impacts the integrity of work performed by government agencies, including financial reporting and public service activities.

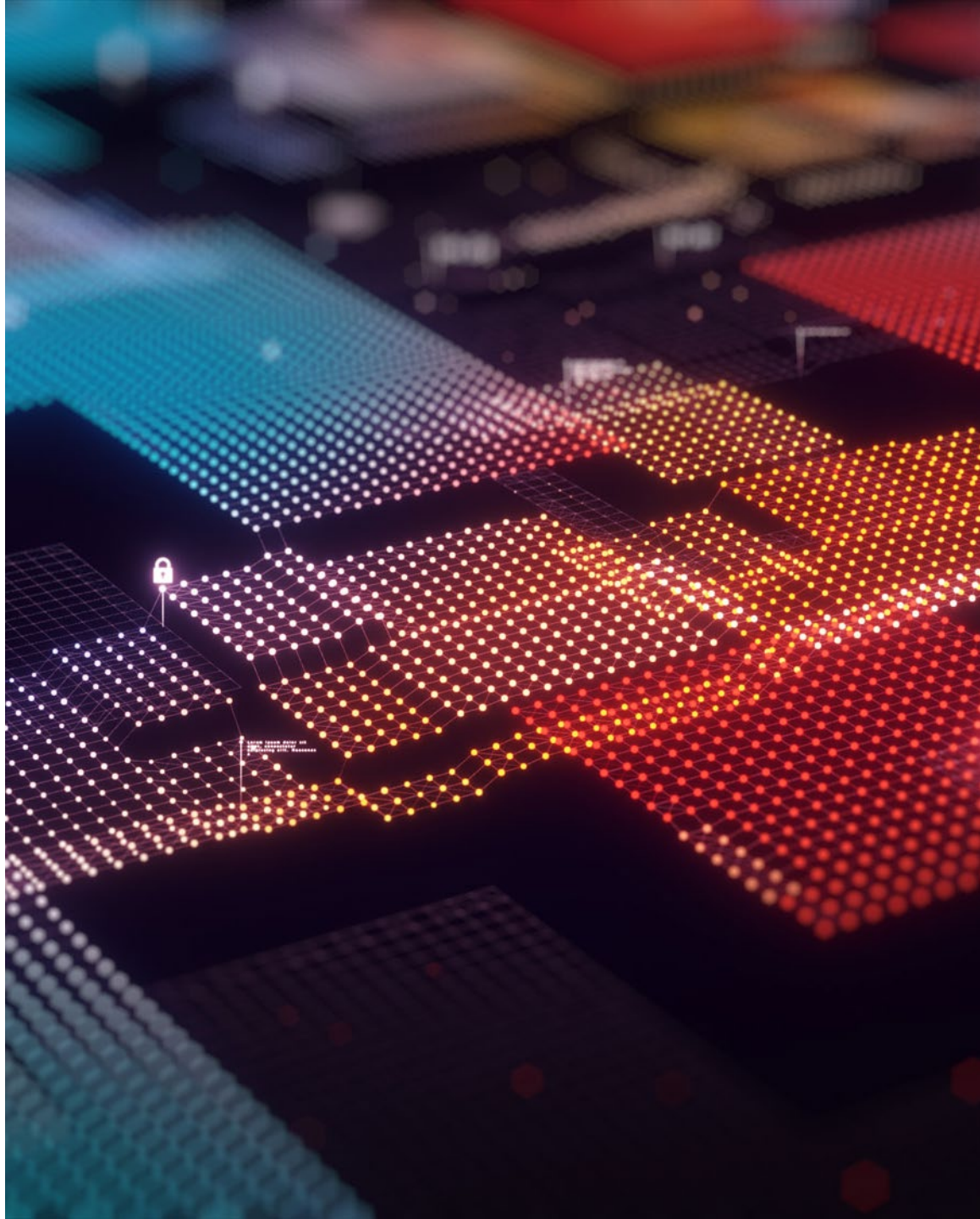
Governments protects critical infrastructure, safeguard sensitive citizen data, and maintain public trust.

Governments often handle sensitive information such as social security numbers, tax information, and voting records.

Challenges including legacy technology, known vulnerabilities, budget constraints, limited staffing, and increased targeting by bad actors.

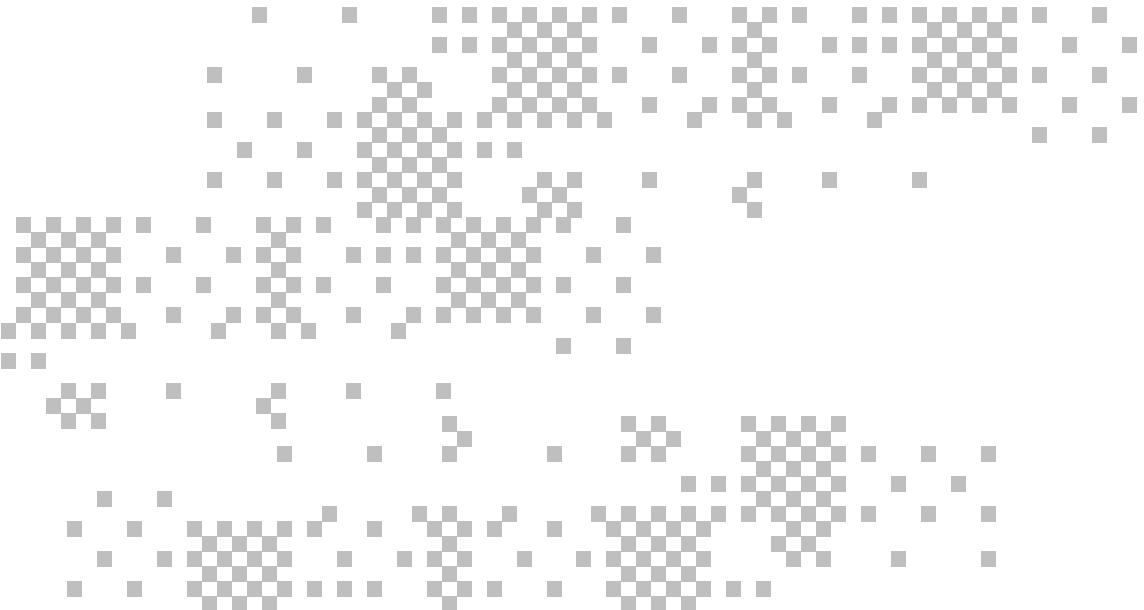
Common IT control findings in government audits

- User access
- Service provider administration
- Backup and contingency planning
- Change management
- Cybersecurity



User access

User access controls help ensure only authorized individuals have access to systems and data, and only at the level needed to perform assigned responsibilities.



Lack of documented approval

Weakness noted:

Government is unable to demonstrate that access requests were formally approved by management or system owners before access was granted.

Related risk:

Users may receive access that is not appropriate or necessary for their job responsibilities.

Missing approvals make it difficult to verify access was properly authorized.

Why do we care?

Unauthorized or excessive access can compromise the integrity of financial data, system processing, or sensitive information.

Recommendation:

Require documented access requests and management approval before access is granted.

Access should not be provisioned until approval is obtained.

Excessive access and least privilege

Weakness noted:

Users are granted access levels that exceed their job responsibilities, often because they inherit access from prior roles or roles are not properly designed.

Related risk:

Users may be able to initiate, approve, and process transactions, particularly in financial systems.

Why do we care?

Excessive access increases the risk of unauthorized transactions, inappropriate changes, errors, or fraud occurring without timely detection.

Recommendation:

Implement role-based access and the principle of least privilege so users receive only the access necessary to perform assigned duties.

Segregation of duties conflicts

Weakness noted:

Users possess incomplete access rights that allow them to both execute and approve transactions and perform multiple stages of a critical process.

Related risk:

A single individual may be able to perform incompatible functions without independent review.

Why do we care?

Segregation of duties conflicts increase the risk of unauthorized, erroneous, or fraudulent transactions.

Recommendation:

Establish a formal segregation of duties matrix identifying incompatible functions and review requested access against the matrix before approval.

Untimely removal of separated employee access

Weakness noted:

Former employees continue to have active accounts after separation because supervisors do not promptly notify system administrators or access is not disabled timely.

Related risk:

Former employees may retain access to systems after separation.

Why do we care?

Active accounts for terminated employees increase the risk of unauthorized access, data compromise, or misuse of agency systems.

Recommendation:

Integrate HR separation notifications with IT processes.

Require account disablement within a defined timeframe.

Compare separated employee listings to active user populations and investigate exceptions.

Inadequate periodic access reviews

Weakness noted:

Management does not conduct or document regular reviews of user access listings to verify access remains appropriate.

Related risk:

Inappropriate access can remain undetected for years, and users may accumulate unnecessary permissions over time.

Why do we care?

Privilege creep can result in users retaining access from prior roles, creating unauthorized access and segregation of duties risks.

Recommendation:

Perform periodic reviews of active accounts, privileged accounts, dormant accounts, and generic IDs.

Document review results and corrective actions.

Monitor inactive accounts and disable or remove them after a defined period.

Privileged accounts

Weakness noted:

Administrator, developer, database, or security administrator accounts are not subject to heightened reviews and monitoring.

Related risk:

Privileged users can alter system configurations, change security settings, or access sensitive data.

Why do we care?

Privilege access has a greater potential impact because it can affect security, system processing, and data integrity.

Recommendation:

Maintain separate approval requirements for administrative accounts.

Periodically review all privileged users.

Policies, populations, and evidence

Weakness noted:

Procedures may not define approvers, documentation standards, onboarding/offboarding timeframes, periodic review requirements, or segregation of duties considerations.

Governments may not be able to produce complete populations of active users, new hires, terminated employees, and privileged users.

Management may lack evidence showing who requested access, who approved it, when access was granted, and when the access was removed.

Related risk:

Management may be unable to effectively monitor access or demonstrate that controls are operating effectively.

Why do we care?

Without complete populations and retained evidence, access controls cannot be validated, monitored, or audited effectively.

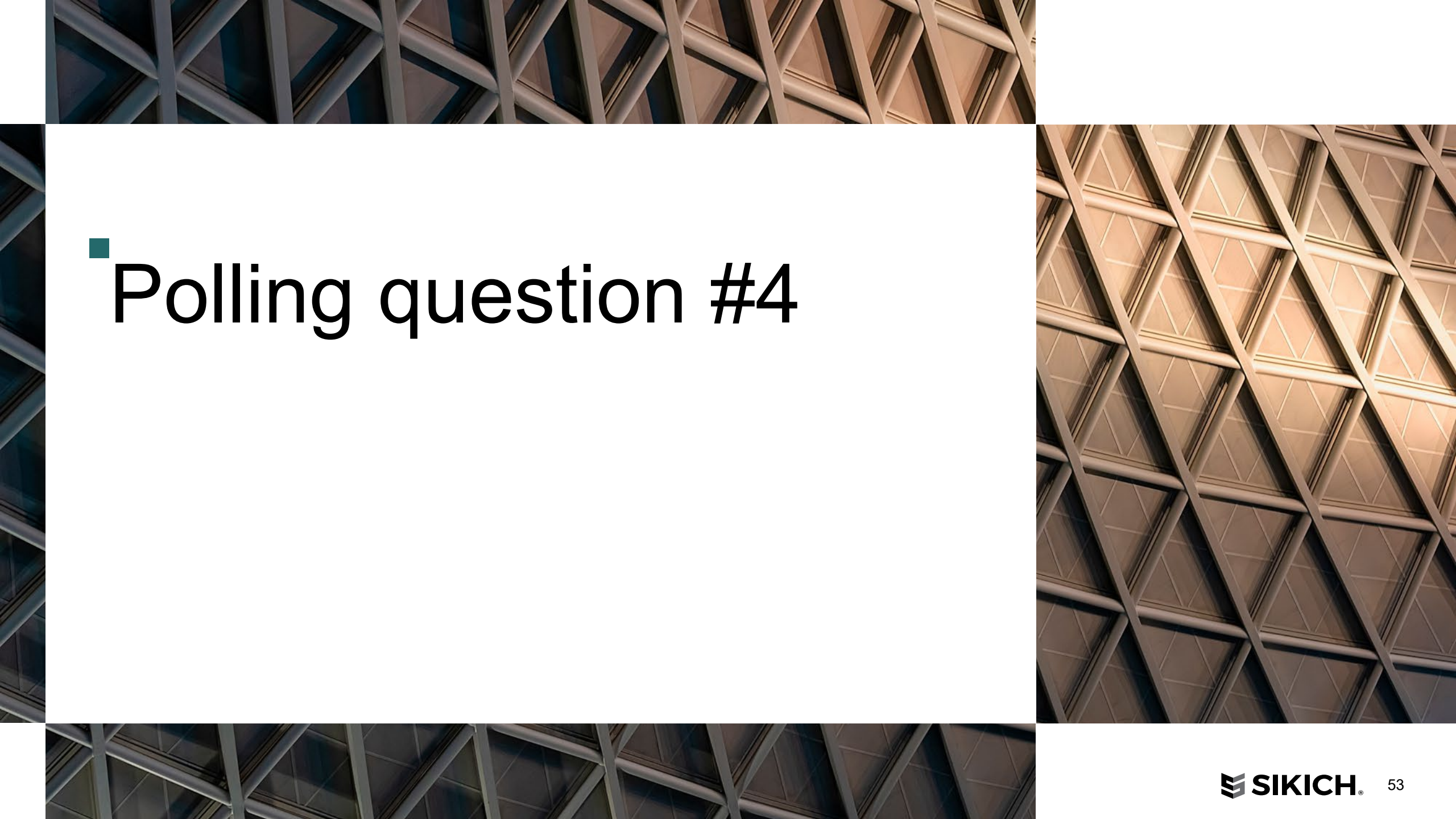
Recommendation:

Develop formal access provisioning policies and procedures.

Generate and retain complete, accurate user populations.

Reconcile user listings to source documents and HR records.

Retain access request forms, approvals, provisioning records, modification records, and separation evidence.



Polling question #4

Service provider administration

Service provider administration weaknesses occur when a government relies on a third party to perform critical services but does not properly monitor, evaluate, or manage the risks associated with that provider.

Failure to assess financial reporting impact

Weakness noted:

Management has not documented how third-party processing activities affect financial reporting controls or identified related risks.

Related risk:

Management may not understand which financial statement accounts, assertions, business processes, reports, or data are affected by each provider

Why do we care?

If outsourced services impact financial reporting, management remains responsible for understanding and monitoring related control risks.

Recommendation:

Maintain a complete inventory of service providers that process financial transactions, host financial applications, generate reports used in financial reporting, or maintain financial/confidential data.

Document service providers, financial data processed, reports generated, accounts affected, significance of outsourced activity, and risks if controls fail.

SERVICE PROVIDER WEAKNESSES

Failure to obtain and review System and Organization (SOC) reports

Weakness noted:

Governments either do not obtain SOC reports or obtain them but fail to perform a documented review.

Related risk:

Management cannot determine whether the service provider's controls operated effectively during the audit period.

Why do we care?

The agency depends on third-party controls, and ineffective provider controls may affect financial reporting, operations, or sensitive information.

Recommendation:

Maintain a complete inventory of service providers and require current SOC 1, SOC 2, or other applicable reports annually.

Review report type, audit period, auditor opinion, exceptions, Complementary User Entity Controls (CUECs), subservice providers, and bridge letters.

Document the review.

SERVICE PROVIDER WEAKNESSES

CUECs, exceptions, and bridge letter

Weakness noted:

Governments may fail to evaluate complementary user entity controls, investigate SOC report exceptions, or obtain/evaluate bridge letters for gaps between SOC report coverage and fiscal year-end.

Related risk:

Management may overlook control responsibilities retained by the agency, qualified opinions, control exceptions, deviations, or gap-period risks.

Why do we care?

Weak service provider administration can result in unauthorized access to confidential or personally identifiable information, inaccurate financial reporting, unidentified third-party control deficiencies, data loss, service interruptions, and noncompliance.

Recommendation:

Perform a documented SOC report review and evaluate opinion, scope, services covered, test results, exceptions, and period covered.

Review exceptions and qualified opinions.

Document management's assessment of the effect on operations and financial reporting.

Obtain and review bridge letters when SOC report periods do not extend through fiscal year-end.

Backup, recovery, and contingency planning

Backup and contingency planning weaknesses occur when a government has not established, maintained, tested, or updated processes necessary to recover systems, applications and data after a cyberattack, natural disaster, or other disruption.

Planning and prioritization

Weakness noted:

Contingency plans are outdated or incomplete.

Related risk:

Recovery procedures may not reflect the current environment, causing delays during an actual disruption.

Why do we care?

Outdated recovery procedures can impair the government's ability to continue critical operations and restore systems timely.

Recommendation:

Develop and maintain comprehensive disaster recovery and business continuity plans and require annual management review and approval.

Planning and prioritization (cont.)

Weakness noted:

No documented business impact analysis.

Related risk:

Critical systems and recovery priorities may not be identified, causing resources to be directed toward less critical functions during an outage.

Why do we care?

Management needs to know which systems and processes must be restored first.

Recommendation:

Conduct periodic business impact analyses to identify critical business processes.

Establish system recovery priorities.

Define recovery time and process objectives.

Backup execution and monitoring

Weakness noted:

Backup procedures are inadequate.

Related risk:

Data may not be recoverable if backup schedules, retention periods, and responsibilities are not clearly defined.

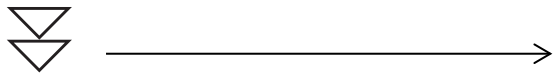
Why do we care?

Without reliable backups, the agency may be unable to restore data needed for operations or financial reporting.

Recommendation:

Establish formal backup procedures defining frequency, retention, storage locations, monitoring responsibilities, and restoration requirements.

Backup execution and monitoring (cont.)



Weakness noted:

Backup procedures are not monitored.

Related risk:

Backup failures may go undetected, resulting in unavailable recovery data when needed.

Why do we care?

Backups only reduce risk if they are successful, complete, and available when needed.

Recommendation:

Review backup logs, investigate failures, and document resolutions.

Periodically report backup performance metrics to management.

Testing and remediation

Weakness noted:

Lack of restoration testing.

Related risk:

Governments cannot demonstrate that backed-up data can actually be restored.

Why do we care?

A backup that cannot be restored does not support recovery.

Recommendation:

Perform and document periodic restoration testing of critical systems and data to validate backup integrity and recovery capabilities.

Testing and remediation (cont.)

Weakness noted:

Disaster recovery testing is insufficient.

Related risk:

Recovery procedures may fail during an actual emergency because they have not been validated.

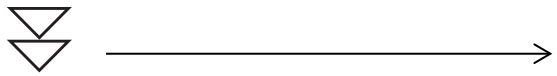
Why do we care?

Testing confirms whether the agency can recover critical systems within expected recovery objectives.

Recommendation:

Conduct annual disaster recovery tests and periodic tabletop exercises that evaluate recovery procedures, system dependencies, and recovery objectives.

Testing and remediation (cont.)



Weakness noted:

Issues identified during testing are not remediated.

Related risk:

Known recovery deficiencies may persist and increase operational risk.

Why do we care?

Testing improves preparedness if findings are tracked and corrected.

Recommendation:

Document test results

Assign corrective action

Track remediation

Perform follow-up testing

Resilience and oversight

Weakness noted:

Offsite or ransom-resistant backups are insufficient.

Related risk:

Backup data may be unavailable if production and backup environments are compromised at the same time.

Why do we care?

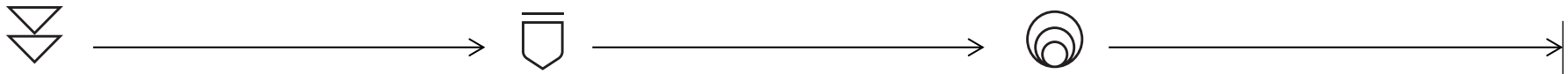
Ransomware and other incidents may affect both primary systems and connected backups.

Recommendation:

Maintain secure offsite, cloud-based, or immutable backups.

Regularly verify backup media protection.

Resilience and oversight (cont.)



Weakness noted:

Roles and responsibilities are undefined.

Related risk:

Recovery efforts may be delayed due to confusion over responsibilities during a disruption.

Why do we care?

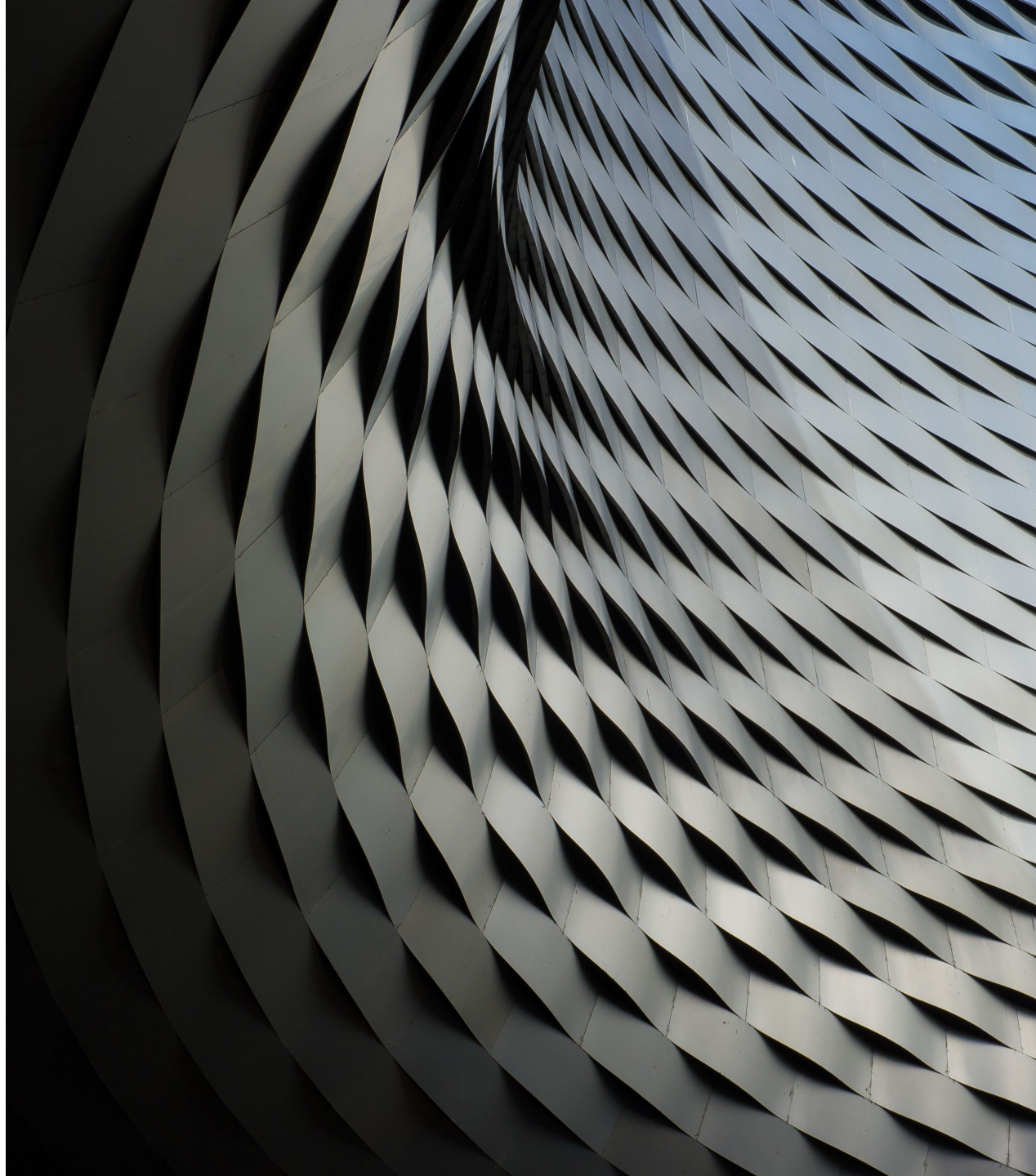
Recovery requires clear accountability, communication, and escalation.

Recommendation:

Define recovery team roles, contact information, escalation procedures, and communication protocols in the contingency plan.

Change management

Change management weaknesses occur when a government does not have adequate controls to ensure changes to applications, databases, operating systems, and infrastructure are authorized, tested, approved, implemented, and documented before migrating to production.



Policies, approval, and testing

Weakness noted:

No formal change management policies and procedures exist.

Related risk:

Changes may be implemented inconsistently and without adequate oversight.

Why do we care?

Inconsistent change practices can result in unauthorized changes, system outages, processing errors, security vulnerability, and inaccurate financial reporting.

Recommendation:

Develop and implement formal policies and procedures covering change requests, approvals, testing, migration, emergency changes, and documentation.

Policies, approval, and testing (cont.)

Weakness noted:

Changes are implemented without documented approval.

Related risk:

Unauthorized or inappropriate changes may be introduced into production environments.

Why do we care?

Unapproved changes can affect system processing, security, and financial data integrity.

Recommendation:

Require documented approval from management and system owners before implementing production changes and retain approved change requests as audit evidence.

Policies, approval, and testing (cont.)

Weakness noted:

Testing prior to implementation is inadequate or evidence of testing is lacking.

Related risk:

New code or system modifications may introduce errors, security vulnerabilities, or processing failures.

Management may be unable to demonstrate changes functioned as intended.

Why do we care?

Untested changes can disrupt financial reporting, operations, and system availability.

Recommendation:

Require testing in a non-production environment.

Document test plans and results.

Resolve identified issues.

Retain approvals before migration to production.

Segregation of duties and production access

Weakness noted:

Developers have direct access to production environments.

Related risk:

Lack of segregation of duties increases the risk of unauthorized or untested changes.

Why do we care?

Direct production access can allow changes to bypass independent review and approval.

Recommendation:

Restrict programmer access to production environments .

Implement compensating monitoring controls when temporary access is required.

Emergency changes, documentation, and follow-up

Weakness noted:

Emergency changes are not formally reviewed.

Related risk:

Emergency changes may bypass normal controls and introduce unrecognized risks.

Why do we care?

Emergency changes may be necessary, but they still require after-the-fact accountability.

Recommendation:

Establish emergency change procedures requiring retrospective testing, approval, and management review after implementation.

Emergency changes, documentation, and follow-up (cont.)

Weakness noted:

Change documentation is incomplete.

Related risk:

Government may not be able to determine why changes were made or whether requirements were met.

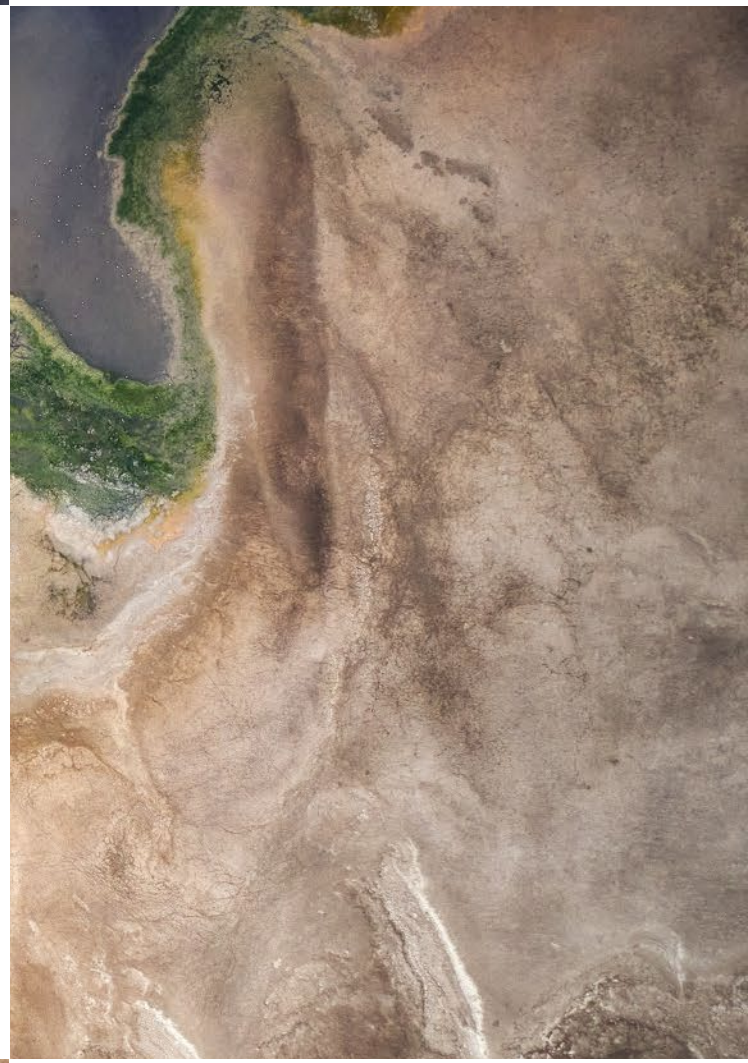
Why do we care?

Complete documentation supports accountability, auditability, validation of change controls.

Recommendation:

Maintain complete records of change requests, approvals, testing, migration dates, and implementation results.

Polling question #5



SIKICH

Cybersecurity

Cybersecurity weaknesses occur when a government has not implemented adequate controls to protect systems, applications, networks, and data from unauthorized access, disruption, modification, or disclosure.

Governance, policies, and risk assessment

Weakness noted:

Lack of comprehensive cybersecurity program.

Related risk:

Security activities may be inconsistent, uncoordinated, or ineffective.

Why do we care?

Without coordinated governance, security responsibilities oversight may be fragmented.

Recommendation:

Establish a formal cybersecurity program defining security responsibilities, risk management processes, security policies, and governance oversight.

Governance, policies, and risk assessment (cont.)

Weakness noted:

Outdated or incomplete security policies and procedures.

Related risk:

Personnel may not follow consistent security practices, increasing exposure to cybersecurity threats.

Why do we care?

Policies define expected security practices and provide a basis for accountability.

Recommendation:

Develop, approve, and periodically review information security policies and procedures covering all major security domain.

Governance, policies, and risk assessment (cont.)

Weakness noted:

Inadequate risk assessments.

Related risk:

Management may be unaware of significant threats and vulnerabilities affecting the organization.

Why do we care?

Risk assessments help management prioritize remediation efforts and resource allocation.

Recommendation:

Conduct periodic cybersecurity risk assessments and use results to prioritize remediation efforts and resource allocations.

Vulnerability management and legacy systems

Weakness noted:

Weak vulnerability management processes.

Related risk:

Known software vulnerabilities may remain unaddressed and exploited by attackers.

Why do we care?

Government systems may be considered soft targets and exploited by bad actors.

Recommendation:

Implement formal vulnerability scanning, patch management, and remediation processes.

Track remediation through completion.

Vulnerability management and legacy systems (cont.)

Weakness noted:

Unsupported or obsolete software and systems.

Related risk:

Legacy technologies may contain vulnerabilities that can no longer be patched by vendors.

Why do we care?

Outdated technology can expose government systems and sensitive data to known threats.

Recommendation:

Replace, upgrade and isolate unsupported systems.

Establish processes to monitor software lifecycle status.

Monitoring and incident response

Weakness noted:

Insufficient security monitoring and logging.

Related risk:

Security incidents may not be detected in a timely manner.

Why do we care?

Delayed detection can allow unauthorized access or system compromise to continue.

Recommendation:

Implement centralized logging, security monitoring and periodic review of security events and alerts.

Training

Weakness noted:

Inadequate employee cybersecurity awareness.

Related risk:

Employees may be more susceptible to phishing, social engineering, and other cyber threats.

Why do we care?

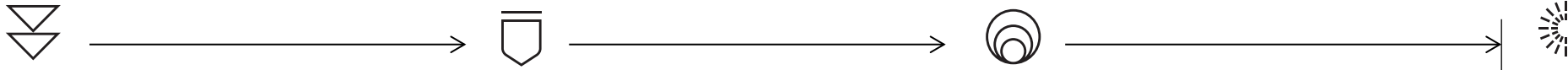
Employees are identified as one of the most common sources of cybersecurity risk. Governments may be unable to demonstrate completion of required training.

Recommendation:

Provide periodic security awareness training and conduct phishing simulations where appropriate.

Require annual training covering phishing, password security, data protection, and incident reporting responsibilities.

Security assessments



Weakness noted:

Failure to periodically assess cybersecurity controls.

Related risk:

Security weaknesses may remain undetected for extended periods.

Why do we care?

Periodic assessments help identify emerging risks and control weaknesses before they result in an incident.

Recommendation:

Perform periodic risk assessments, penetration testing, vulnerability assessments, internal reviews, independent evaluations, and management reviews to identify and address control weaknesses.

IT control findings

Why cybersecurity weaknesses are significant

- Cybersecurity controls protect the confidentiality of information, integrity of systems and data, and availability of critical service.

Cybersecurity weaknesses

Potential consequences when controls are ineffective:

- Data breaches
- Unauthorized access
- System outages
- Financial loss
- Regulatory noncompliance
- Disruption of critical government services

IT control weaknesses

Common themes:

- Controls are often not formally documented.
- Management approval and oversight are often missing or not retained.
- Reviews may be performed inconsistently or not evidenced.
- Complete populations are necessary to support monitoring and audit testing.
- Segregation of duties and privileged access require heightened attention.
- Testing, follow-up, and remediation are critical for backup, contingency, change management, and cybersecurity controls.

IT control findings

Governments should:

- Formalize policies and procedures
- Define ownership
- Retain evidence
- Perform periodic reviews
- Monitor exceptions
- Document corrective actions

88

SAS No. 145 overview and application

SAS No. 145

- Why are we talking about SAS No. 145?

What has changed?

Before SAS No. 145

- Risk assessments often became routine
- Procedures frequently rolled forward from year to year
- Technology understanding varied significantly

What has changed?
(cont.)

After SAS No. 145

- Greater emphasis on understanding risks
- More focus on IT systems and automated processes
- Better linkage between risks and audit procedures
- Increased documentation of auditor judgments

What has changed? (cont.)

Client impact - more discussion about:

- Business processes
- IT systems
- Internal controls
- Changes in operations

SAS No. 145

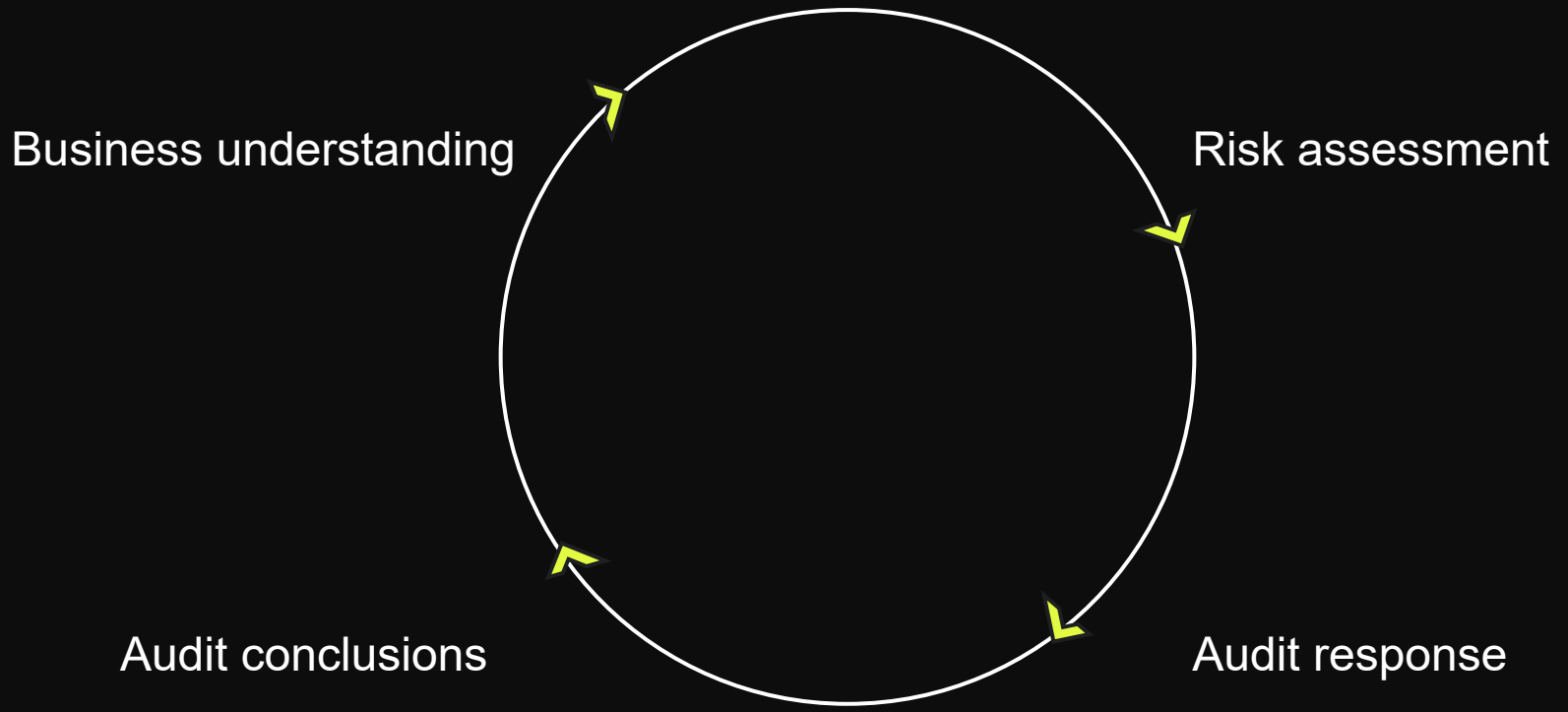
What we have learned:

- Risk assessment is no longer just a title of a planning form – it drives the entire audit.

Why it matters:

- Auditors must identify risks, evaluate those risks, and design procedures that specifically address those risks.
- Clients benefit from more targeted testing, increased audit effectiveness, and better focus on significant areas.

SAS No. 145


Business understanding
Risk assessment
Audit conclusions
Audit response

SAS No. 145

- One of the most significant changes is that auditors must assess inherent risk before considering controls.
- Inherent risk is what could go wrong naturally because of complexity, judgment, estimates, change, and/or fraud exposure.
- Auditors are spending more time understanding where mistakes could occur.

SAS No. 145

Technology is now a central focus. (cont.) approval, and testing

What we have learned:

- Most financial reporting processes rely heavily on technology.

Areas receiving greater attention

- User access
- Change management
- Service providers
- Automated controls
- Backup and recovery process

SAS No. 145

Technology is now a central focus.
approval, and testing

Why do we care?

- Weak IT controls can affect:
  - Data integrity
  - Completeness of transactions
  - Financial statement accuracy

SAS No. 145

Why are auditors requesting more information? Approval, and testing

SAS No. 145 requires auditors to understand:

- How transactions flow through systems
- Who performs reviews
- How errors are identified
- How controls operate
- How technology supports financial reporting

The questions are designed to help us understand risk, not simply collect documentation.

SAS No. 145

Why this is good for client organizations?

A stronger risk assessment can:

1. Improve audit quality through a better understanding of risks and audit responses.
2. Improve audit efficiency by focusing testing where risks are greatest and reduce unnecessary procedures in lower-risk areas.
3. Improve organizational insight by developing a better understanding of processes and identification of control weaknesses and opportunities for process improvement.

SAS No. 145

Is this really new?

The concepts existed before, but SAS No. 145 expanded and clarified expectations.

SAS No. 145

What have we learned?

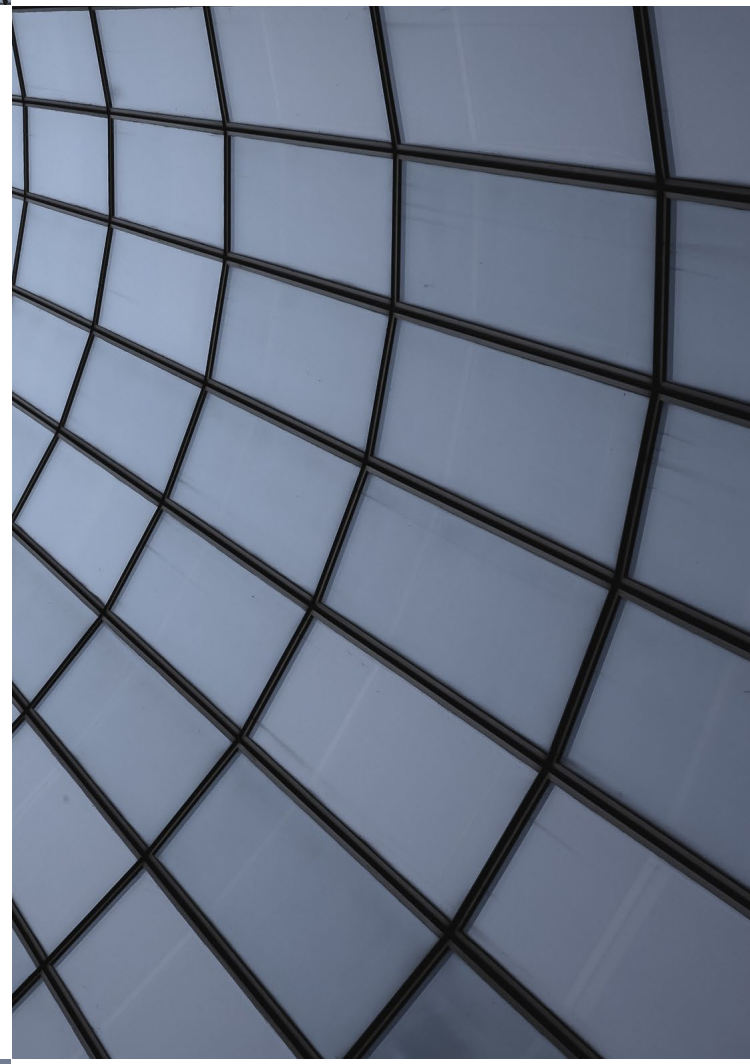
- Risk assessment is now the centerpiece of the audit.
- Technology risks deserve significant attention.
- Understanding controls improves audit quality.
- Better risk assessment leads to better audit procedures.
- The goal is not more work – it is smarter work.

SAS No. 145

What have we learned? (contd.)

SAS No. 145 was designed to improve audit quality by helping auditors gain understanding of an organization's operations, controls, and technology environment so that audit procedures are focused on the risks that matter most.

Polling question #6



Question?

Anthony Cervini, CPA, CFE

Principal

anthony.cervini@sikich.com

Amy Sherwood, CPA, CISA

Principal

amy.sherwood@sikich.com

Thank you

Sikich practices in an alternative practice structure in accordance with the AICPA Professional Code of Conduct and applicable law, regulations, and professional standards. Sikich CPA LLC is a licensed CPA firm that provides audit and attest services to its clients, and Sikich LLC and its subsidiaries provide tax and business advisory services to its clients.

Sikich CPA LLC has a contractual arrangement with Sikich LLC under which Sikich LLC supports Sikich CPA LLC's performance of its professional services. Sikich LLC and its subsidiaries are not licensed CPA firms. "Sikich" is the brand name under which Sikich CPA LLC and Sikich LLC provide professional services. The entities under the Sikich brand are independently owned and are not liable for the services provided by any other entity providing services under the Sikich brand. The use of the terms "our company", "we" and "us" and other similar terms denote the alternative practice structure of Sikich CPA LLC and Sikich LLC.

SIKICH®