



Louisville Kentucky | September 14-18, 2025



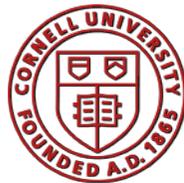
Value Proposition of Root Cause Analysis (RCA)

From Symptoms to Solution



Mark Perry

Chief Audit Executive
MBA; CPA, CIA, CFE
mark.perry@cornell.edu



Cornell University



Curt Josey

Associate Director, Analytics & Data Strategy
MBA(c), MEng; CIA, CISA, ACDA
curtis.josey@cornell.edu

Learning Objectives

Understand value proposition of root cause analysis (RCA)

Describe sustainable RCA strategies for internal audit

Summarize alternative approaches for complex issues

Identify key RCA elements of the Global Internal Audit Standards

Institute of Internal Auditors (IIA) Guidance

2025 IIA Global Internal Audit Standards

Standards require Chief Audit Executive (CAE) to drive strategic alignment, collaboration, quality improvement and transformation.

- 1. Standard 8.1 concerning Board interaction(s)**
the CAE should share insights around themes, which will require an understanding of root causes
- 2. Standard 9.3 on IA methodologies**
the CAE must establish methodologies for all key IA activities, which will include root cause analysis
- 3. Standard 9.4 on the Internal audit plan**
highlights that the rationale for engagements must be clear and explicitly refers to root cause(s)
- 4. Standard 11.3 concerning communicating results**
this *can* include root causes and best practices
- 5. Standards 14.3 and 14.4 the evaluation of findings and recommendations and action plans**
these provide clearest requirements for RCA including workpaper requirements

https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards_2024january9.pdf



Engagement-Level RCA Guidance

2025 IIA Global Internal Audit Standards

Internal auditors are expected to apply structured Root Cause Analysis methods as part of audit engagements

Standard 14.3 Evaluation of Findings

14.3 REQUIREMENTS

Internal auditors must evaluate potential engagement finding to determine its significance. When evaluating potential engagement findings, **internal auditors must collaborate with management to identify the root causes *when possible***, determine the potential effects, and evaluate the significance of the issue.

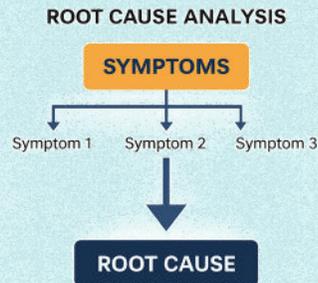
Standard 14.4 Recommendations and Action Plans

14.4 REQUIREMENTS

Internal auditors must determine whether to develop recommendations, request action plans from management, or collaborate with management to agree on actions to:

- Resolve [differences from established criteria]
- Mitigate identified risks to an acceptable level
- **Address the root cause of the finding**
- Enhance or improve the activity under review

What is Root Cause Analysis (RCA)?



Root Cause Analysis (RCA)

- structured approach to **identifying underlying causes or control failures**
- **RCA enables more effective risk mitigation** by addressing the source
- Thematic RCA should be communicated to the board and senior mgmt.
- RCA aims to identify what went wrong, *not who is at fault*

CHARACTERISTICS OF ROOT CAUSE



Underlying reason



Not immediately visible



Unlikely to recur

Characteristic(s)

- may not be immediately visible (unlike observable symptoms)
- requires analysis to identify
- when addressed, problem is unlikely to recur
- complex issues may have more than one root cause

METHODS OF ROOT CAUSE ANALYSIS



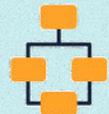
5 Whys



Pareto Rule



Ishikawa Diagram



Nadler-Tushman Congruence Model

Common Internal Audit RCA Approaches

- 5 Why's Method: simple and easy, higher variability
- Pareto Rule: requires more data, less variability
- Ishikawa (Fishbone) Diagram: useful to identify multiple root causes
- Nadler-Tushman Congruence Model: strategic organizational misalignment

Methods: 5 Whys



Overview

An iterative interrogative approach of RCA to explore cause and effect, repeating “why?” 5+ times at prior answer.

If the same issue would be reasonably prevented, mitigated, or detected based on correcting the root cause, stop.

If not, keep going or try another approach.

Originated in 1930s by the founder of Toyota Industries.

Pros

- **Easy and intuitive to apply with few resources**
- Sustainable option throughout fieldwork
- Easy to pivot to more advanced methods
- Stop when answer is an internal control ‘light switch’
if addressed problem unlikely to recur
(preventative > detective > directive controls)

Example

Finding: manager approval not recorded

1. *Why?* No monitoring or enforces it.
2. *Why?* Process is not automated.
3. *Why?* Process is undocumented.
4. *Why?* Manager not aware it should be required.
5. *Why?* Gaps in job role hiring, onboarding, and training.
→ **gaps in business continuity plans**
→ **lack of accountability (‘tone at the top’)**

Cons

- **Outcomes may vary based on individuals involved**
- Oversimplification of complex issues may miss RCA
- Management may attempt to steer into ‘visible issues’
(e.g., vacant position issue vs accountability)

Methods: Pareto Rule (20% cause 80% issues)

Overview

List, classify and map data available on causes over time.

Chart data looking for most common cause over time.

Focus on areas causing approximately 80% of problem.

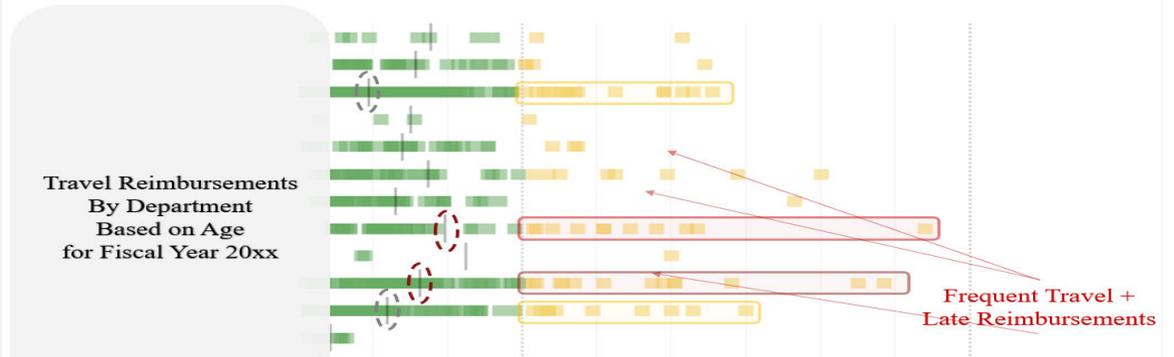
Originated in 1896 by Vilfredo Pareto, refined in 1940s.

Pros

- **Ideal for long-term issues with sufficient data**
- Works well in continuous assurance programs
- More repeatable process transferrable to management
- Prioritized outcomes

Example

Insight Example: Late Travel: 80% from 20% of Dept's



Cons

- **Requires sufficient qualitative data**
- **Approach is more retrospective than future focused**
- Limited applicability – situational dependent

Methods: Ishikawa (Fishbone) Diagram

Overview

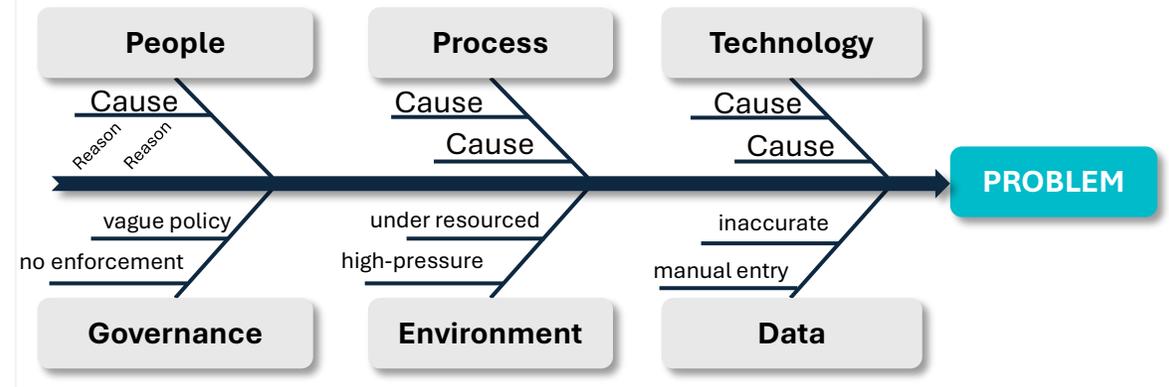
Requires a clearly defined problem, thinking through categories of causes through brainstorming session(s), mapping out the cause and effect across contributing factors.

Invented in 1940s by Kaoru Ishikawa for continuous process improvement (aka '6 Ms' in Manufacturing: Method, Machinery, Material, Manpower, Measurement, Mother Nature).

Pros

- **Visually links cause-and-effect relationships**
- **Facilitates collaboration in problem-solving**
- Generate innovative solutions
- May identify multiple root causes for remediation plans
- Can easily integrate with 5 Whys (e.g., for each cause)

Example



Cons

- **Easily side-tracked into sub-issues and too many ideas**
- More complicated due to number of factors to consider
- Classifications add further complexity and time sinks
- May result in more fieldwork and/or observations

Methods: Nadler-Tushman Congruence Model

Overview

Views organizations as interacting components that *should* exist in relative harmony with each other - aka congruence.

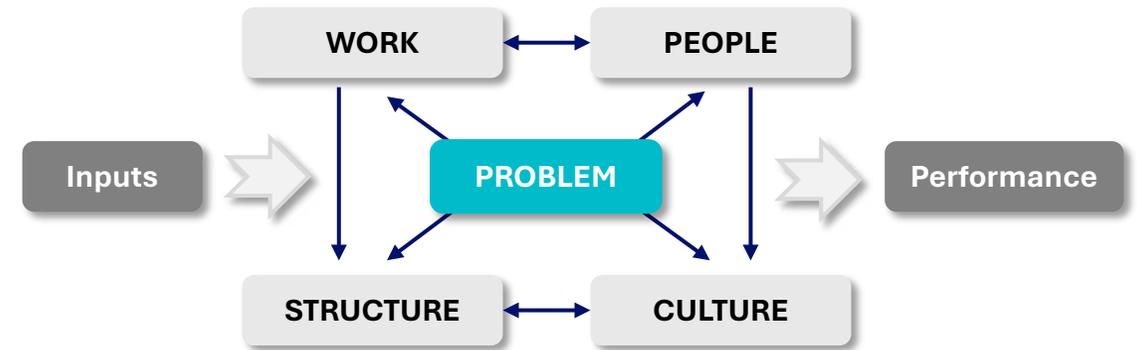
- **Work:** are tasks performed consistent w/ objectives?
- **People:** are they motivated, skilled, qualified?
- **Structure:** does org. structure inhibit success?
- **Culture:** informal constructs on acceptable behaviors
- **[Implied]:** interdependencies requiring collaboration

Originated in 1980s from a Business Executive and a Columbia University prof.

Pros

- **Strategic insight that might otherwise be missed**
- **Alignment focused (e.g., identifies misalignments)**
- Focus on diagnostic work before recommendations
- Helps identify root cause barriers to change, useful for transformation audits and post-implementation reviews

Example



Cons

- **Complex to apply for small issues**
- **Time consuming for full analysis and can add delays**
- Data intensive across multiple dimensions
- Subjectivity risk when evaluating culture/leadership

Challenges to Avoid



Pitfall	Avoid By
Assumptions	Applying structured methods to analyze
Addressing Only Symptoms	Ask deeper questions on underlying risk drivers
Bypassing Management / Limited Perspectives	Engage all key stakeholders to get holistic view
Confirmation Bias	Encourage open discussion and questioning
Decisions with Incomplete Data	Collect and use qualitative and quantitative data
“Pointing Fingers”	Focus RCA on internal control issues
Unsustainable Process	Keep simple as possible, as complex as necessary
Zero Tolerance for Imperfection	Allow time to learn, get more data, fail-forward

Using COSO (2013) for RCA

The COSO Internal Control Integrated Framework is a common and useful tool for developing and assessing internal controls and for conducting RCA.

The COSO Framework is comprised of 5 Components and 17 underlying Principles and additional 87 Points of Focus. It applies to all entity objectives and activities.

It can be incorporated into any of the RCA methods described herein. *Remember to consider all aspects of the Framework when assessing RCA.*



Build an RCA Toolbox



The Best Method?

The best method will vary based on the situation, data, personnel, skills, time, and other factors.

Tips

- RCA effort should be proportionate to the risk
- Start simple as possible, as complex as necessary
- Leverage “AI” to self-assess potential root causes¹
- Perform in small groups to gain more local perspective
- Always consider detective and preventative controls
- Involve clients early on, as part of regular fieldwork
- Use the RCA output to enhance recommendations
- Draft observations / RCA should not be a surprise

Establish RCA Strategic Roadmap

- Create supporting templates and ‘cheat sheets’
- Introduce RCA concepts at engagement kickoff
- Lead group RCA exercises using past audit(s)
- Maintain library of well-known and agreed upon RCAs
- Align w/ COSO Internal Control – Integrated Framework
- Transfer RCA concepts with 2nd line of assurance
- Track common RCA overtime to identify thematic issues
- Periodically report themes to senior leadership / board



Align “AI” use of non-public data with institutional “AI” governance due to data privacy, information security, and hallucination risks.

RCA integration w/ Internal Audit Activities

2025 IIA Global Internal Audit Standards

RCA supports conformance with IIA principles of insight, objectivity, and governance.

Engagement Integration

Scoping

- Review past engagements for potential unaddressed root causes
- Educate auditors and management on RCA concepts

Fieldwork

- On-going, internal RCA discussion with peers, management (e.g., informal 5 Whys - detection failure?, prevention failure?)
- In regular client meetings explore potential causes & gauge responses

End of Fieldwork

- Review findings, RCA to confirm understanding and client perspectives
- **Consider separate RCA *if* significant findings lack agreed cause**

Reporting

- Ensure observations issued address all significant RCA
- During close-out meeting, confirm understanding and acceptance
- If appropriate, highlight root cause themes in executive summary

Strategic Integration

Charter

- Consider addressing RCA methodologies and expectations

Internal Audit Work Plan

- Consider systemic & common root causes during audit work planning
- Review enterprise risk management – risk log for potential RCA themes

Continuous Assurance

- Incorporate RCA into continuous control test results (e.g., Pareto Rule)

Quality Assurance Improvement Program (QAIP)

- Periodically sample RCA output for future improvement/training
- Periodically sample follow-up results to validate RCA addressed
- Update catalog of common, agreed upon RCA and occurrence rates

Senior Leadership and the Board

- **Standard 11.3, Communicating Results** on RCA themes and trends to improve organizational learning, governance, and strategy (e.g., collaborate with enterprise risk management, report to board)

RCA Sample Scenario

Common Internal Audit RCA Approaches

- 5 Why's Method: simple and easy, higher variability
- Pareto Rule: requires more data, less variability
- Ishikawa (Fishbone) Diagram: useful to identify multiple root causes
- Nadler-Tushman Congruence Model: strategic organizational misalignment

Facilitate Group Workshops

“Inadequate Documentation of Year-End Account Reconciliation”

Findings

- A. Policy requires management to perform periodic account reconciliations
- B. Management attests they do perform account reconciliations on a regular and on-going basis
- C. Management attests the reconciliation process is not documented nor monitored
- D. Management attests the person responsible left the position after the period under review
- E. Management attests they lack resources to fill the vacant position

Questions

1. What RCA approach would you select? Why?
2. Would additional information be required for the RCA? Explain response.
3. What is the most likely root cause based on available information. Why?

AI Example Prompt

Play the role of an internal auditor performing root cause analysis using the following technique: **[method]**.
Flag any information provided that seems overly critical or biased.
Suggest a better root cause method if appropriate.
Explain all responses.
Ask questions to improve results.



Consider creating an internal audit “AI prompt library” to improve efficiency, consistency, and repeatability of the most useful AI prompts.

Prompt Library

Q Search

Findings currently known, include:

[findings list]



- A. Policy requires management to perform periodic account reconciliations
- B. Management attests they do perform account reconciliations on a regular and on-going basis
- C. Management attests the reconciliation process is not documented nor monitored
- D. Management attests the person responsible left the position after the period under review
- E. Management attests they lack resources to fill the vacant position

Assessed finding is **[risk level]**.

Summarize responses in concise, layperson terminology, and suggest potential preventative, mitigating, or detective controls that are likely to be cost effective and efficient based on the observed risk.



Align “AI” use of non-public data with institutional “AI” governance due to data privacy, information security, and hallucination risks.

AI Example Response

✦ Applying Nadler-Tushman Model

Let's explore each element and ask questions to uncover deeper causes:

1. WORK (Tasks and Processes)

- **Known Issue:** Reconciliation is required but not documented or monitored.
- **Questions:**
 - What does the reconciliation process actually involve?
 - Is there a standard template or checklist used?
 - How is reconciliation frequency determined?
- **Observation:** Lack of documentation suggests **process fragility and inconsistency**.

3. STRUCTURE (Reporting Lines, Accountability)

- **Known Issue:** No monitoring of reconciliation.
- **Questions:**
 - Who was responsible for oversight?
 - Is there a control owner or reviewer role defined?
 - Are reconciliations tied to performance metrics or KPIs?
- **Observation:** **Weak accountability structure** may allow the process to lapse unnoticed.

2. PEOPLE (Skills, Roles, Capacity)

- **Known Issue:** The responsible person left, and the role is unfilled.
- **Questions:**
 - Was the person trained or certified in reconciliation?
 - Is there cross-training or backup coverage?
 - What prevents hiring or reallocating resources?
- **Observation:** Staffing gaps and **lack of redundancy are contributing factors**.

4. CULTURE (Values, Norms, Priorities)

- **Known Issue:** Management attests to doing reconciliations but lacks evidence.
- **Questions:**
 - Is there a culture of “trust without verification”?
 - Are controls seen as burdensome or optional?
 - How does leadership respond to control gaps?
- **Observation:** **Potential cultural bias toward informal practices over formal controls**.

🛡️ Suggested Controls (Cost-Effective & Efficient)

MITIGATING CONTROLS

- **Temporary reassignment** of reconciliation duties.
- **Use shared services or external support** until role filled.
- **Risk-based prioritization** of accounts to reconcile.

IMMEDIATE ACTION(S)

PREVENTATIVE CONTROLS

- **Documented procedures** with clear steps & responsibilities.
- **Cross-training** to ensure backup coverage.
- **Role definition** in job descriptions and onboarding materials.

SUSTAINABLE SUCCESS PLAN

DETECTIVE CONTROLS

- **Automated reconciliation logs** or audit trails.
- **Periodic review by finance leadership** or internal audit.
- **Exception reporting** for missed reconciliations.

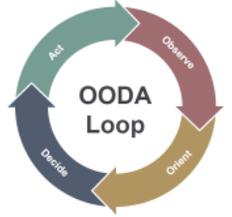
OVERSIGHT & MONITORING ACTION(S)

❓ Is Nadler-Tushman the Best Fit?

This model is useful for **organizational alignment**, but if the issue is more **process-specific**, a **Fishbone (Ishikawa) Diagram** or **Five Whys** might better isolate technical, human, and control-related causes.

WARNING: Results shown are for illustrative purposes, most modern “AI” model responses are subject to change over time – even when using same inputs.

Key Takeaways



Value



RCA facilitates observations designed to support *sustainable* organizational success
→ moving beyond symptoms to comprehensive, future-focused solutions

Expect more comprehensive observations, offset by fewer repeat issues over time
→ when combined with periodic RCA thematic / trend analysis and reporting

Embrace a culture of learning from mistakes, or a ‘fail forward’ mentality
→ expect a learning curve, complex issues may benefit from dedicated facilitation

Impact



Trusted Advisor

Robust RCA will enhance perceptions of internal audit’s capabilities and impact
→ may bring a measured increase in advisory and consulting service requests

Board Engagement

RCA insights may bring greater engagement with board and senior leadership
→ enables more focus on the highest risks; “*What really keeps you up at night?*”

Thank You

Presenters

Mark Perry, MBA; CPA, CIA, CFE

Chief Audit Executive

Cornell University

mark.perry@cornell.edu

Curt Josey, MBA(c), MEng; CIA, CISA, ACDA

Associate Director, Analytics & Data Strategy

Cornell University

curtis.josey@cornell.edu

Collaborators

AuditCon Planning Committee (acua.org)

- Katrina McNair
- John McDaniel

Cornell University (cornell.edu)

- Elizabeth Mannix, PhD, Organizational Theory
- Risa Mish, JD, *Critical Thinking*

Diligent (diligent.com)

- Katja Freeman kfreeman@diligent.com
- Andrea Walsh awalsh@diligent.com

Appendix

Additional supporting materials

Appendix: Common Root Cause Library

#	Root Cause Reason	Example	Control Type	ERM Component	DOJ 7 Elements
1	Access Control	Unrestricted access to sensitive data or physical assets.	Preventative	Control Activity	Internal Controls
2	Audit Trail/Log	insufficient records to trace transactions or events	Detective	Info. & Comm.	Monitoring & Auditing
3	Authorization Control	lack of clear approval processes or exceeding authorized limits	Preventative	Control Activity	Internal Controls
4	Change Management	failure to properly assess and control changes to systems, processes, or personnel affecting internal controls	Corrective	Risk Assessment	Risk Assessment
5	Communication	lack of clear and timely communication of control-related information	Directive	Info. & Comm.	Communication & Training
6	Continuous Improvement	failure to regularly review / update controls based on changes in business, technology, or risk profile	Corrective	Monitoring Activities	Monitoring & Auditing
7	Control Ownership	unclear assignment of responsibility for specific controls	Preventative	Control Environ.	Governance & Oversight
8	Control Testing	inadequate testing of control design and operating effectiveness	Detective	Monitoring Activities	Monitoring & Auditing
9	Data Integrity	use of unreliable or inaccurate data in control processes	Corrective	Info. & Comm.	Internal Controls
10	Documentation	Absence of clear, documented procedures and policies creates unnecessary business continuity risk	Preventative	Info. & Comm.	Policies & Procedures
11	Follow-up Procedure	failure to ensure that corrective actions are effective	Corrective	Monitoring Activities	Corrective Action
12	Hiring/Training	Inadequate vetting of new hires, or insufficient employee training on control procedures	Preventative	Control Environ.	Communication & Training
13	Inefficient Process(es)	Unnecessarily complexity in control procedures leads to inefficiency	Corrective	Risk Assessment	Risk Assessment
14	Monitoring Activity	Infrequent or inadequate monitoring of key controls	Detective	Monitoring Activities	Monitoring & Auditing
15	Organizational Culture	a culture that does not prioritize effective internal controls or ethical behavior	Directive	Control Environ.	Governance & Oversight
16	Outlier/Variance Analysis	failure to investigate significant deviations from expected results	Detective	Risk Assessment	Risk Assessment
17	Reconciliation	failure to regularly compare records or investigate discrepancies	Detective	Monitoring Activities	Monitoring & Auditing
18	Resource Allocation	inadequate staffing or funding for control activities	Directive	Risk Assessment	Governance & Oversight
19	Review/Assessment	absence of periodic reviews by independent parties can lead to preventable blind spots in assessments	Detective	Monitoring Activities	Monitoring & Auditing
20	Root Cause Analysis	failure to determine the underlying reasons for control failures	Corrective	Risk Assessment	Corrective Action
21	Segregation of Duty	when one employee has control over all phases of a transaction (authorization, recording, custody).	Preventative	Control Activity	Internal Controls

DISCLAIMER: Data is for illustrative purposes only, showing ability to crosswalk potential root causes across key risk frameworks for integrated assurance reporting.

Appendix: Links to Related Resources

- Clinical Excellence Commission. Pareto Charts & 80-20 Rule.
<https://www.cec.health.nsw.gov.au/CEC-Academy/quality-improvement-tools/pareto-charts>
- Diligent. COSO internal control framework: What it is & how to use it
<https://www.diligent.com/resources/blog/coso-internal-controls-framework>
- Diligent. Explore Diligent's AI offerings: solutions, software features and expert insights (GRC with purpose-built AI).
<https://www.diligent.com/lp/machine-learning-artificial-intelligence-in-governance-audit-risk-compliance>
- Diligent. Solutions for Higher Education.
<https://www.diligent.com/industries/higher-education>
- Diligent. Leveraging technology to tackle the DOJ's 7 elements.
<https://www.diligent.com/resources/blog/doj-elements-of-effective-compliance>
- Harvard Business School. Understanding the Congruence Model: Aligning Strategy, Structure & People.
<https://online.hbs.edu/blog/post/congruence-model>
- Institute of Internal Auditors. Common Root Causes - Linked to Internal Control-Integrated Framework.
<https://internalauditor.theiia.org/globalassets/site/magazine/articles/2022/digging-deep/2206cosochart.jpg>
- Institute of Internal Auditors. Getting Started With: Root Cause Analysis (RCA): Podcast Video.
<https://www.theiia.org/en/content/podcast/getting-started-with/2025/ep-0024/>
- Institute of Internal Auditors. Global Internal Audit Standards.
https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards_2024january9.pdf
- Institute of Internal Auditors. The Root of the Matter: Performing root-cause analysis requires that auditors recognize common myths associated with the process.
<https://fie.is/wp-content/uploads/2017/09/ia201707-dl.pdf>
- OWASP. Top 10 Risk & Mitigations for LLMs and Gen AI APPs.
<https://genai.owasp.org/>
- Texas Department of State Health Services. Root Cause Analysis – Fishbone Template.
<https://www.dshs.texas.gov/sites/default/files/hivstd/qm/files/FishboneDiagramTemplate.doc>

Appendix: 5 Whys Examples

Budget overruns in research grant

1. **Why** did the department exceed its research grant budget?
→ Because several expenses were not properly tracked or approved.
2. **Why** were expenses not properly tracked or approved?
→ Because the department used manual spreadsheets instead of the university's financial system.
3. **Why** did they use manual spreadsheets?
→ Because staff found the financial system difficult to use and time-consuming.
4. **Why** was the financial system difficult to use?
→ Because staff were not trained adequately on how to use it for grant management.
5. **Why** were staff not trained adequately?
→ **There is no formal training program for onboarding financial system users in research departments.**

Unauthorized access to student data

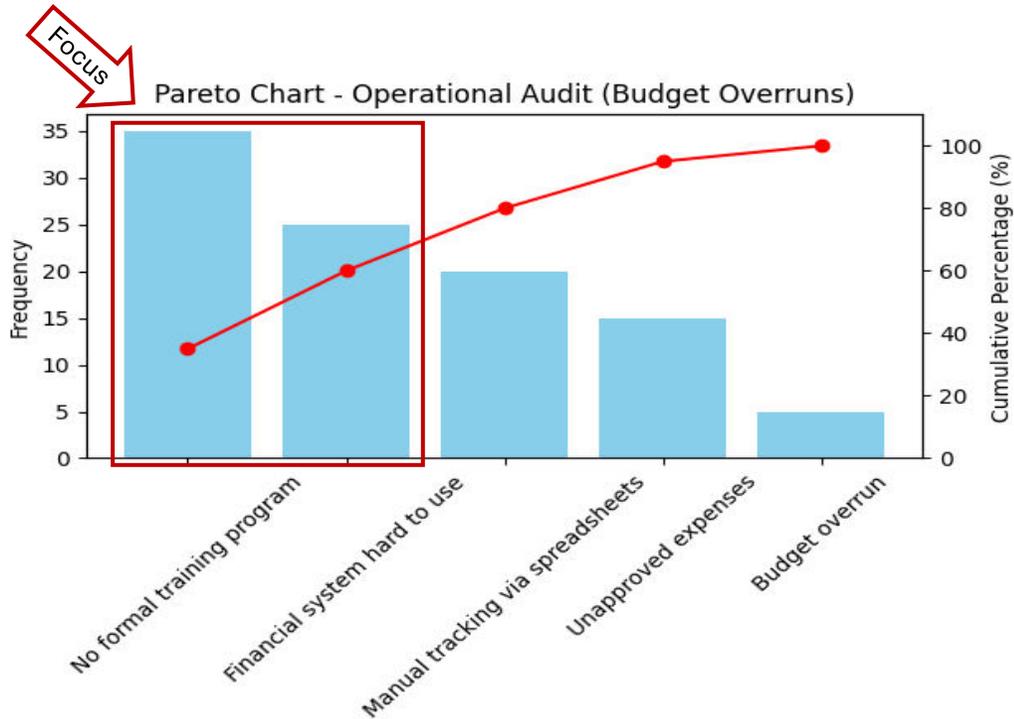
1. **Why** was student data accessed by unauthorized users?
→ Because user accounts were compromised.
2. **Why** were the accounts compromised?
→ Because passwords were weak and reused across systems.
3. **Why** were weak passwords allowed?
→ Because the system didn't enforce strong password policies.
4. **Why** didn't the system enforce strong password policies?
→ Because IT security settings were outdated and not aligned with current standards.
5. **Why** were security settings outdated?
→ **There is no formal process for periodic security reviews and updates.**

... [may require further RCA exploration on culture/oversight]



Appendix: Pareto Rule Examples

Budget overruns in research grant



Unauthorized access to student data

