ROOT CAUSE ANALYSIS IN COMPLEX, TECH-DRIVEN ENVIRONMENTS

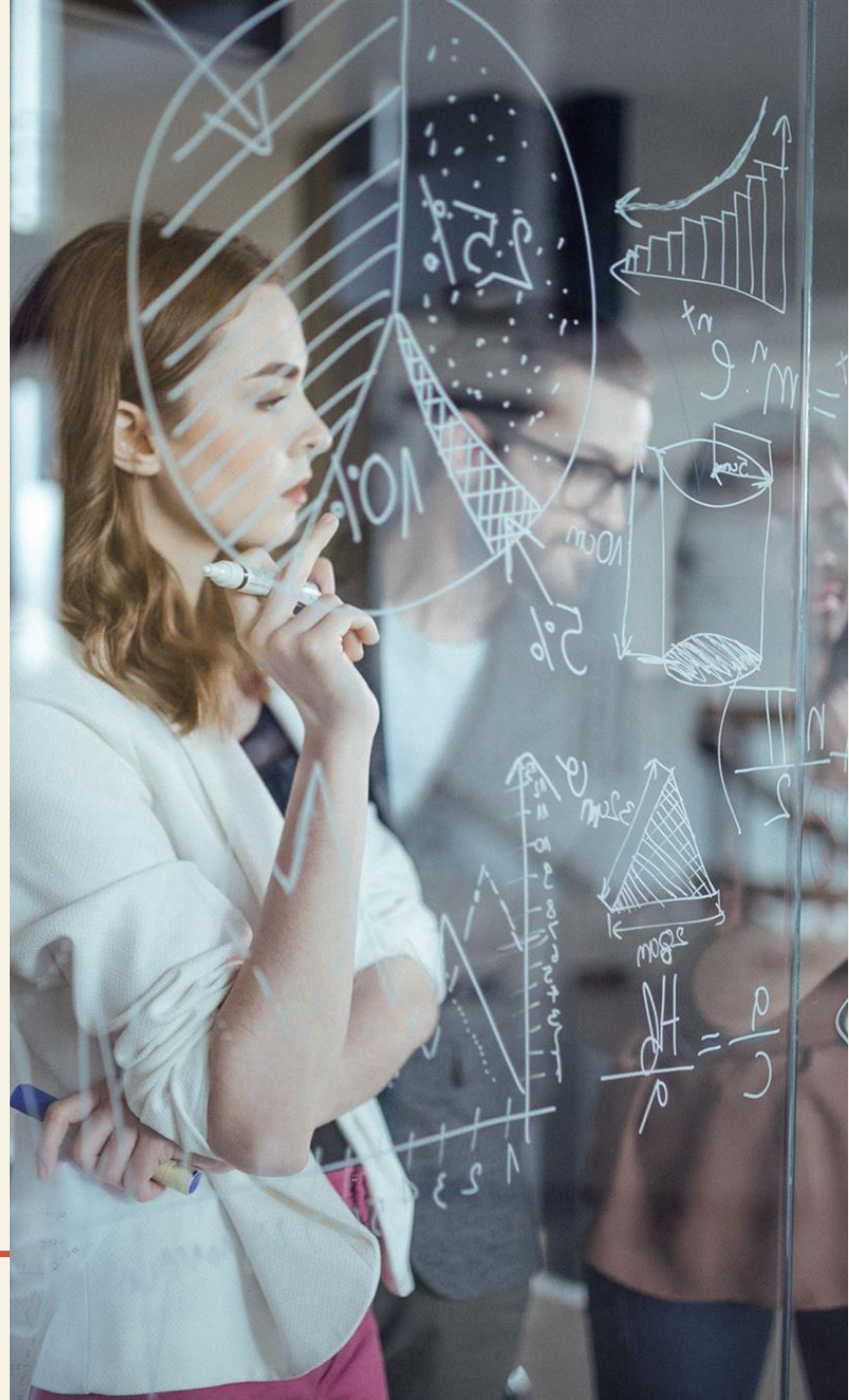
Uncovering underlying issues in advanced technological systems

GLC

POLL 1

WHAT IS ROOT CAUSE ANALYSIS (RCA)?

- Structured approach to **identifying underlying causes or control failures**.
- Aims to identify **what went wrong**, not who is to blame.
- May not be immediately visible and require analysis.
- When **addressed**, prevents recurrence.
- Complex issues may have **multiple root causes**.
- Key root causes should be communicated to the **Board** and **Senior Management**.



WHY RCA MATTERS FOR INTERNAL AUDIT

RCA Role

RCA is essential for auditors to identify underlying causes beyond surface symptoms in complex systems.

Enhancing Audit Value

Embedding RCA transforms internal audit into an advisory role, supporting strategic remediation and continuous improvement.

Impact on Risk Management

Applying RCA improves organizational resilience through actionable insights and strengthens risk management.

Standards and Compliance

IIA standards require auditors to drive strategic alignment, collaboration and quality improvement to address root causes.

WHY RCA MATTERS FOR INTERNAL AUDIT

Standard 8.1 concerning Board interaction(s)
the Chief Audit Executive (CAE) should share insights around themes, which will require an understanding of root causes

Standard 9.3 on IA methodologies
the CAE must establish methodologies for all key IA activities, which will include root cause analysis

Standard 9.4 on the Internal audit plan
highlights that the rationale for engagements must be clear and explicitly refers to root cause(s)

Standard 11.3 concerning communicating results
this *can* include root causes and best practices

Standards 14.3 and 14.4 the evaluation of findings and recommendations and action plans
these provide clearest requirements for RCA including workpaper requirements

POLL 2

KEY RCA METHODS FOR TECHNOLOGY CONTEXTS

5 Whys

An iteractive interrogative approach of RCA to explore cause and effect, repeating “why?” 5+ times at prior answer.
Best Used in isolated control or process failures.

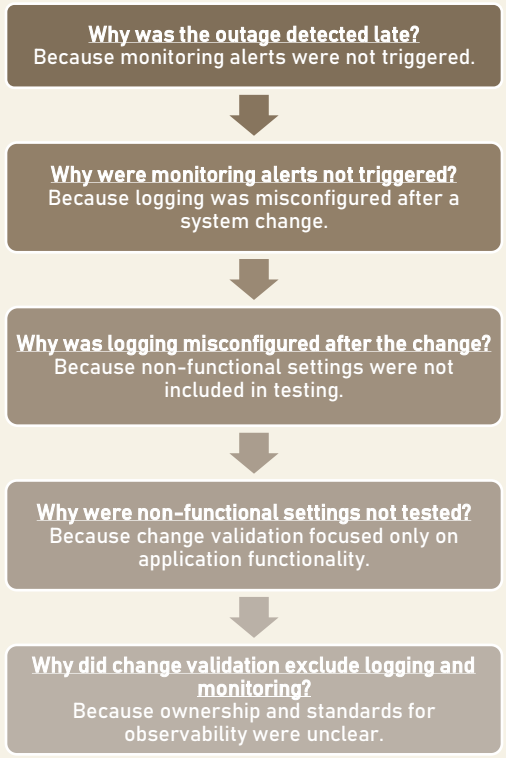
Key Pros

Simple and fast; minimal data required

Key Cons

High variability; may oversimplify complex issues

Problem:
A cloud-based core system outage was detected late.



Root Cause:
Lack of clear ownership and governance over monitoring and change validation.

KEY RCA METHODS FOR TECHNOLOGY CONTEXTS

Ishikawa (Fishbone)

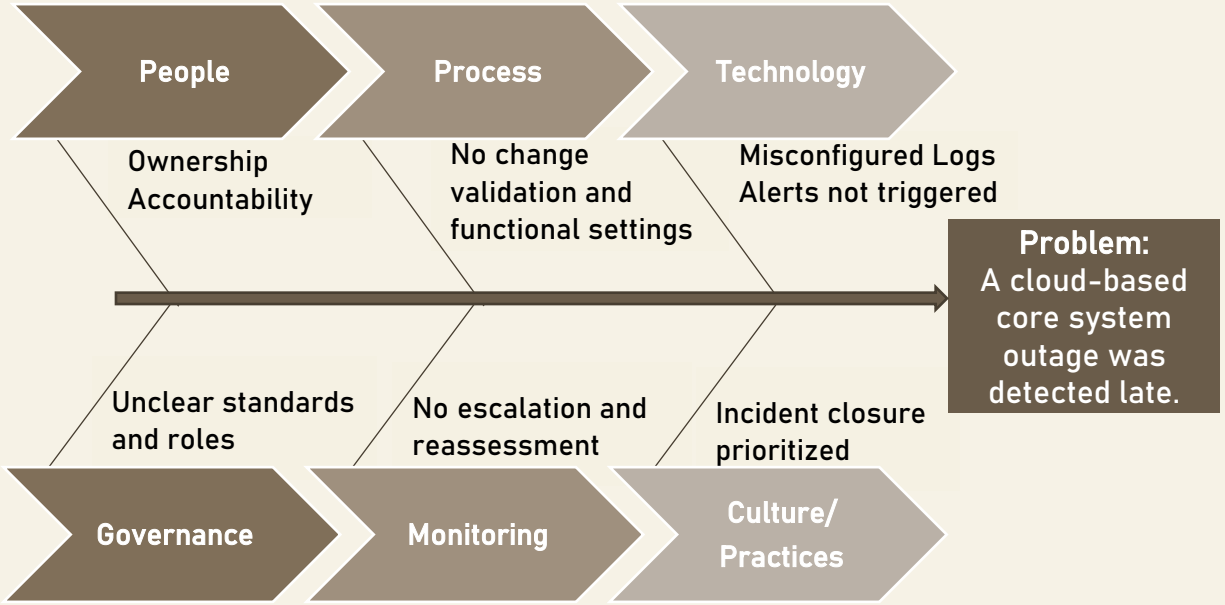
Mapping out the cause and effect across contributing factors.
Can have Multiple technical and non-technical contributors.

Key Pros

Identifies multiple root causes; strong visual mapping; collaborative.

Key Cons

Can become complex and time-consuming



KEY RCA METHODS FOR TECHNOLOGY CONTEXTS

Pareto Rule

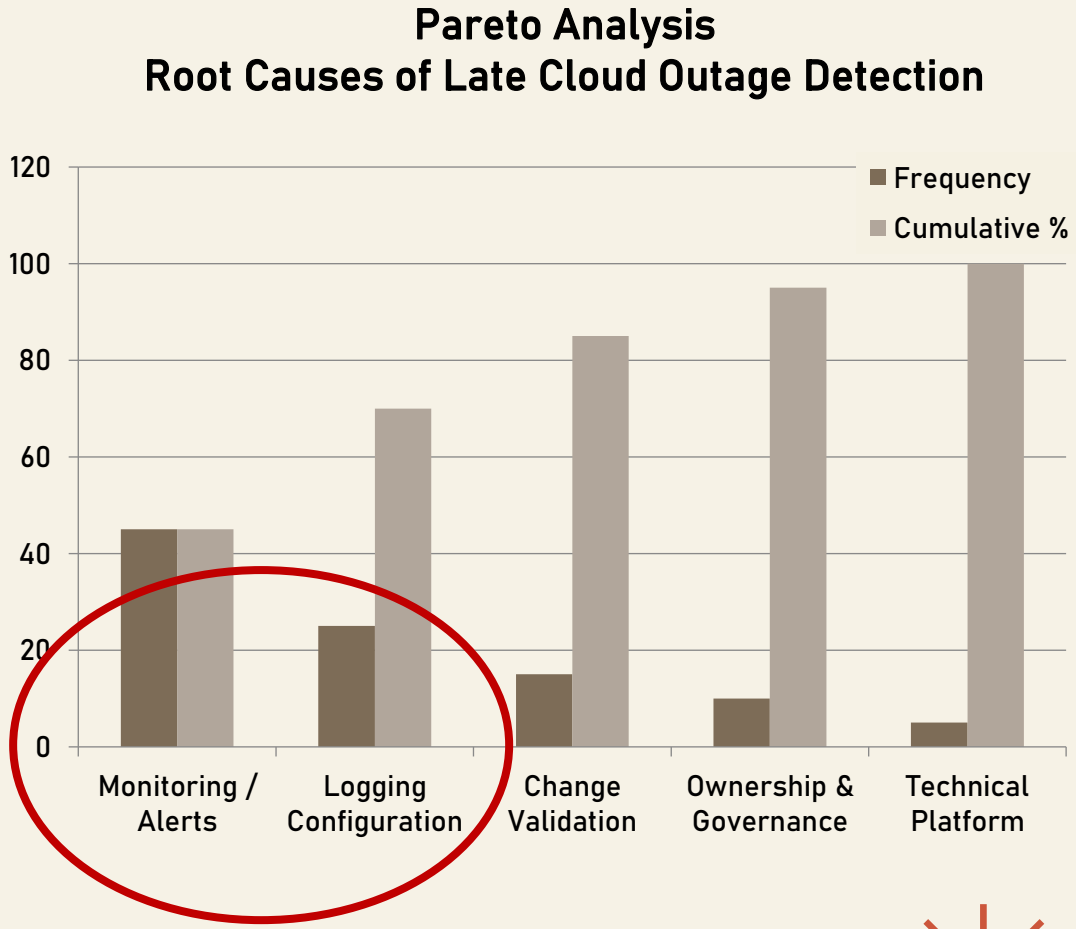
List and categorize causes using historical data, using trends to identify the most frequent causes. Prioritize causes responsible for roughly 80% of issues.

Key Pros

Prioritizes most impactful causes; supports trend analysis.

Key Cons

Data-dependent; retrospective focus.



KEY RCA METHODS FOR TECHNOLOGY CONTEXTS

Risk Bow-Tie Analysis
Links causes, controls, and consequences.

Key Pros
Highlights preventive, detective, and recovery control gaps.

Key Cons
Needs facilitation and Subject Matter Expert (SME) input.

Threats / Causes:
Logging misconfigured
Monitoring alerts disabled
Non-functional testing missing
Unclear monitoring ownership

Consequences:
Delayed incident response
Extended downtime
Regulatory exposure
Reputational impact

Problem:
A cloud-based core system outage was detected late.

Preventive Controls:
Change management
Configuration validation
Monitoring standards

Detective & Recovery Controls:
Alerts & dashboards
Escalation procedures
Incident response

KEY RCA METHODS FOR TECHNOLOGY CONTEXTS

Nadler–Tushman Congruence Model

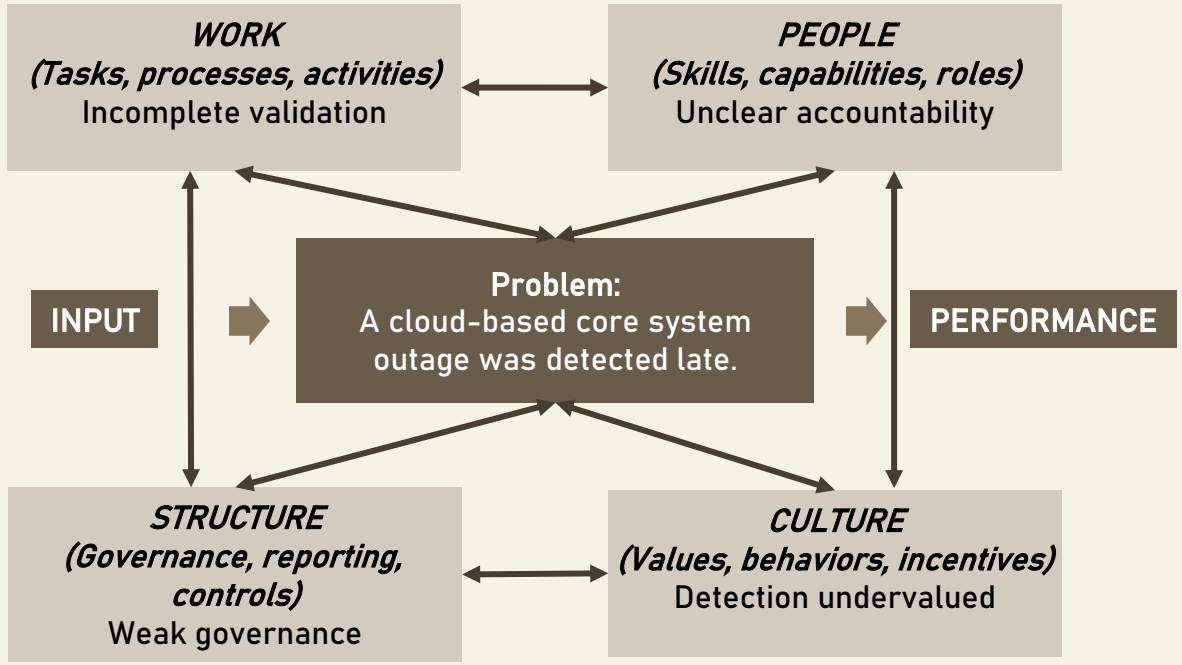
Helps identify misalignment between organizational elements driving systemic failures.

Key Pros

Strong strategic insight; identifies structural and cultural gaps

Key Cons

Complex; overkill for small issues



KEY RCA METHODS FOR TECHNOLOGY CONTEXTS

Fault Tree Analysis (FTA)

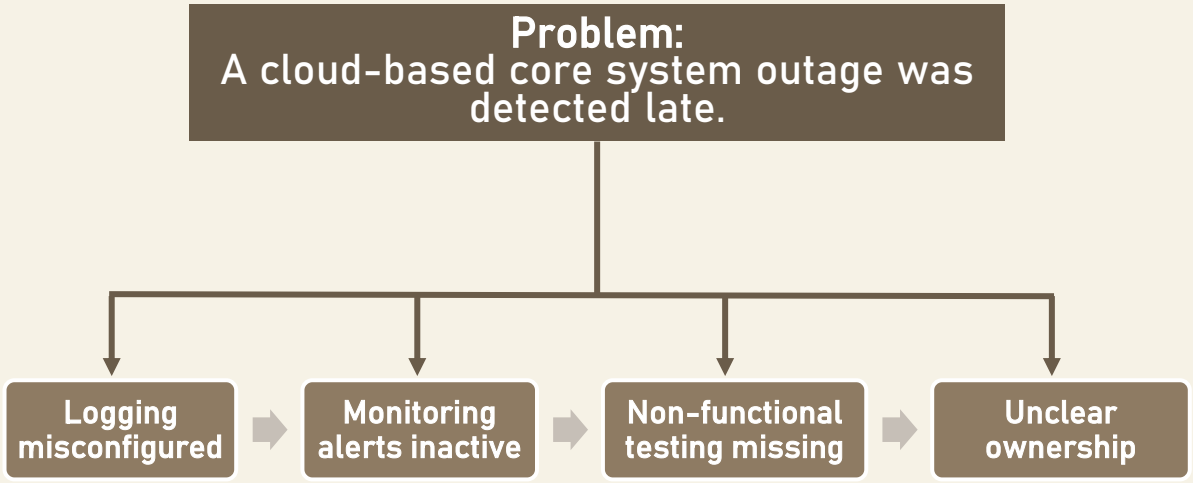
Top-down, structured method used to analyze how multiple failures and control breakdowns combine, through logical relationships, to cause a specific undesired event.

Key Pros

Explains how multiple failures combine using AND/OR logic

Key Cons

Requires analytical discipline; less intuitive without facilitation



CHALLENGES TO AVOID IN RCA (TECH ENVIRONMENTS)

Key Challenges	5 Whys	Fishbone	Bow-Tie	FTA
Stopping at symptoms	✓	✓		
Assumption-driven analysis	✓	✓		
Pointing to people or tools	✓	✓		
Tool over process dependency	✓	✓	✓	
Ignoring combined failures			✓	✓
Overlooking support configurations (logging/monitoring)	✓	✓	✓	✓
Limited perspectives		✓	✓	
Treating learning as optional	✓	✓		
Focusing only on delivery (ignoring lifecycle)		✓	✓	
Fragmented ownership	✓	✓	✓	
Letting standards drift	✓	✓		
Using the wrong RCA method				✓

CHALLENGES TO AVOID IN RCA EXAMPLES FOR TECH ENVIRONMENTS

IAM weaknesses treated as execution errors

Initial root cause evaluation: Explaining access control deficiencies as workload or operational issues.

Evidence from audit

- Re-certification not performed at required frequency
- Privileged accounts without documented review or expiry
- Shared accounts used without governance or clear accountability

What RCA revealed

- Processes perceived as time-consuming
- IAM focus limited to high-risk systems
- Fragmented ownership across applications

RCA Tools used:

5 Whys: Uncover why governance, prioritization, and accountability are insufficient for IAM controls.

Ishikawa (Fishbone): Analyze contributing factors across process scalability, tooling, roles, and governance.

FTA: Evaluate when IAM risks were materialized due to multiple governance and control failures.

AI SUPPORT TO RCA EXECUTION

AI Example Prompt:

Act as an Internal Auditor certified by the Institute of Internal Auditors (IIA), with expertise in reviewing processes related to **[audit subject]** . Perform a structured root cause analysis using the **[specified method]** (e.g., 5 Whys, Fishbone/Ishikawa, or Fault Tree Analysis).

Critically assess the information provided and flag any statements that appear **biased, unsupported, or overly judgmental.**

Evaluate whether the selected root cause methodology is appropriate; if not, **recommend a more suitable approach and justify your choice**.

Clearly **explain your reasoning at each step**, ensuring transparency and logical consistency in the analysis.

Identify underlying root causes, distinguishing them from symptoms or contributing factors.

Ask targeted follow-up questions, where needed, to refine the analysis and improve accuracy. Consider the findings below: **[findings list]**

Conclude by:

Summarizing the identified root causes in a clear and structured manner.

Recommending **practical and cost-effective controls**, categorized as **preventive, detective, and/or mitigating, aligned** with the level of risk observed **[issue grading definitions]**

Classify Root Cause **[root cause categories]**

.

POLL 3

INVESTIGATING FAILURES IN AUTOMATED ENVIRONMENTS

- Automation reduces manual errors but introduces hidden, systemic failure risks
- Failures propagate rapidly across integrated systems, platforms, and dependencies
- Processes may continue running while producing incorrect or incomplete outputs
- Misconfiguration, biased outputs, and automation misuse create unseen vulnerabilities

INVESTIGATING FAILURES IN AUTOMATED ENVIRONMENTS

Key challenges in automated environments

- Over-reliance on automated controls
- Silent failures with no immediate alerts
- Automation and AI introduce new vulnerabilities faster than controls adapt
- Insufficient oversight and exception handling/validation

INVESTIGATING FAILURES IN AUTOMATED ENVIRONMENTS

Real Case — RPA Bot Failures

What happened
An RPA bot supporting a critical process failed repeatedly and required frequent restarts.

Initial explanation
“Bot instability” or “tool limitation”

What RCA revealed

- Exception handling was not designed into the bot logic
- Input validation did not cover real-world data variability
- No monitoring existed to detect recurring exception patterns (Pareto Rule)

RCA methods used

- ✓ **Fishbone (Ishikawa):** identified design, data, monitoring, and governance gaps
- ✓ **5 Whys (multi-leg):** separated prevention failures (design) from detection failures (monitoring)
- ✓ **Thematic RCA:** confirmed recurring automation design weaknesses across bots

POLL 4

LEVERAGING LOG DATA & SYSTEM AUDITS

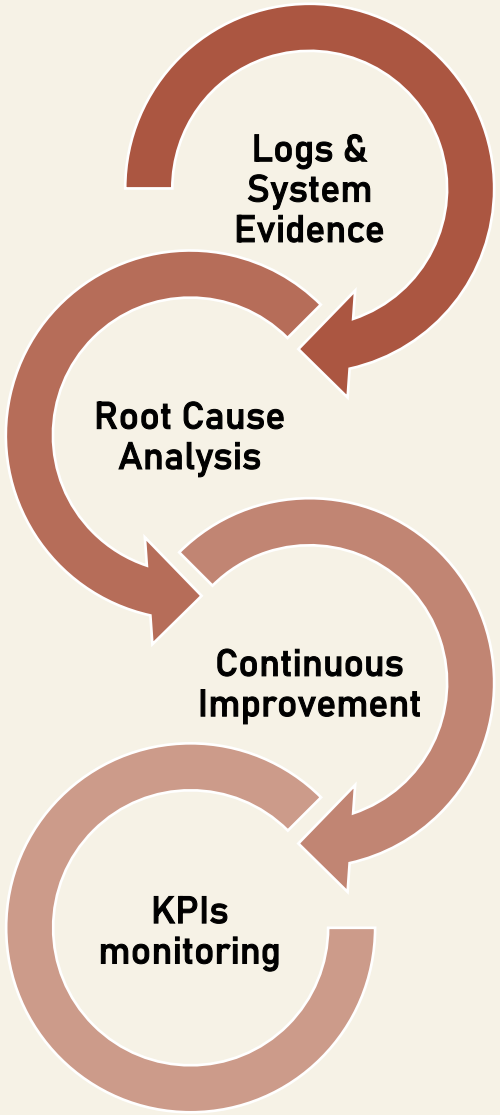
Why log data matters

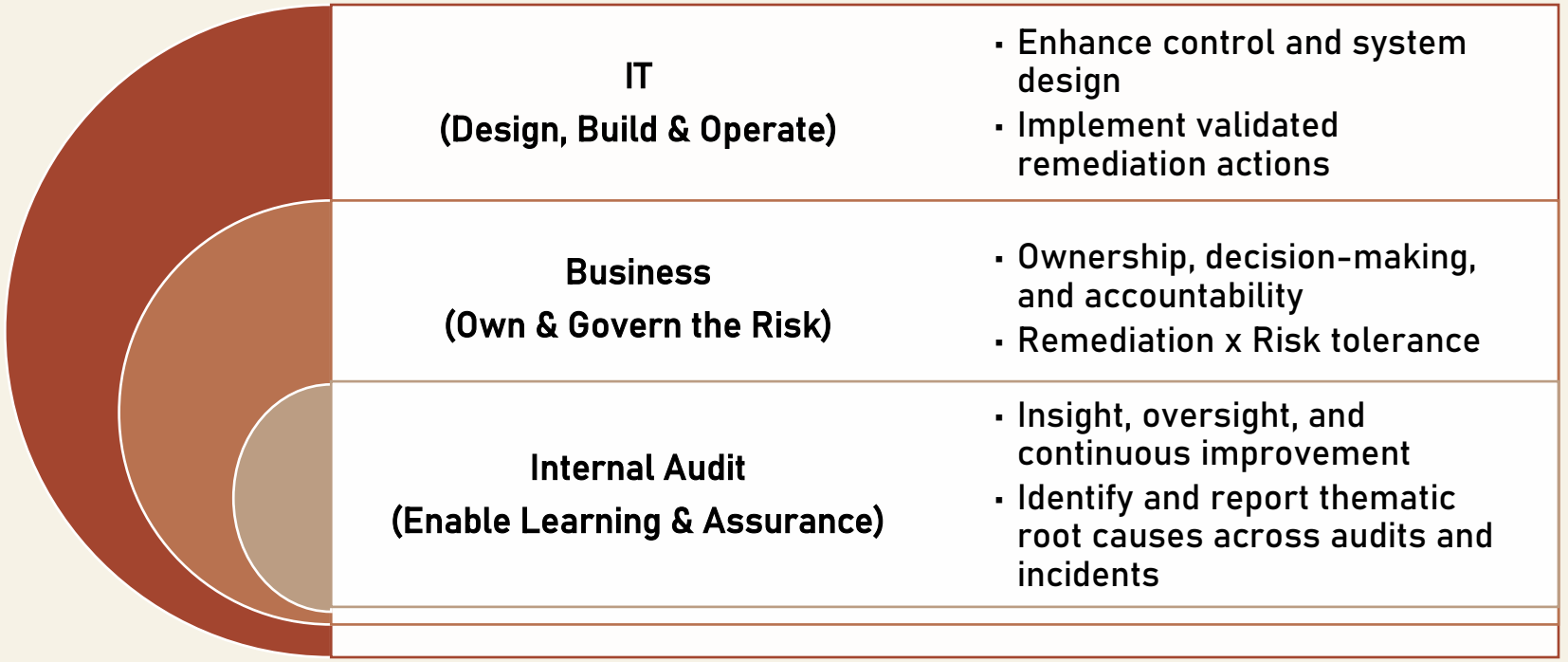
- Logs provide objective, time-stamped evidence of system behavior
- They enable auditors to move from assumptions to facts
- Logs reveal not only what failed, but when controls failed to detect or prevent

What to focus on as an IT auditor

- **Completeness:** Are critical events logged (errors, access, changes)?
- **Integrity:** Are logs protected from alteration?
- **Timeliness:** Are logs reviewed during the risk window?
- **Actionability:** Do alerts trigger investigation and escalation?

CONTINUOUS IMPROVEMENT INTEGRATION





IT **(Design, Build & Operate)**	▪ Enhance control and system design ▪ Implement validated remediation actions
Business **(Own & Govern the Risk)**	▪ Ownership, decision-making, and accountability ▪ Remediation x Risk tolerance
Internal Audit **(Enable Learning & Assurance)**	▪ Insight, oversight, and continuous improvement ▪ Identify and report thematic root causes across audits and incidents

Key RCA-Driven KPIs

- Reduction in repeat findings
- Time to detect failures (via logs/alerts)
- Time to remediate root causes
- Most common root causes

FROM INCIDENTS TO SUSTAINABLE IMPROVEMENT

- Technology incidents are rarely caused by a single technical error
- Most failures arise from systemic weaknesses in design, monitoring, governance and ownership
- Logs & System Evidence reveal what happened and when it happened
- Sustainable improvement requires evidence-based RCA, not symptom fixes
- Continuous Improvement drives control redesign, stronger monitoring, and reduced recurrence

THANK YOU!

ANNE BARBOSA, CIA

Internal Audit Manager at Generali Seguros

linkedin.com/in/annecsb