Proving Program Effectiveness

From Documentation to Demonstrated Resilience

Canadian National Conference

RESILIENCE by Design

Session Agenda

1. What Is A Paper Tiger?
2. Defining Program Effectiveness
3. Why This Matters Now
4. Levels of Effectiveness & The Pressures That Test It
5. The Assessment: Five Systems x Five Criteria
6. Applying The Assessment To Real Cases
7. Reporting Effectiveness To The Audit Committee
8. One Move To Start
9. Questions

Canadian National Conference

RESILIENCE by Design

Learning Objectives

- Distinguish between documented compliance & demonstrable program effectiveness under stress.
- Apply an antifragility-informed model to evaluate governance & compliance programs beyond checklist assurance.
- Develop board-ready reporting that demonstrates accountability, depth & resilience.

Canadian National Conference

RESILIENCE by Design

“A paper tiger”

The CFO Was Right

- My program confirmed the controls existed and operated; it never asked whether they would hold against someone determined to defeat them
- We never screened the vendor master against officers' interests; we never hunted for override patterns
- The only warning came from a person, not from the program, and that person paid for it

What follows is the answer I have spent the years since then building.

Who Finds It

43%

of occupational fraud detected by tips

ACFE 2026

~15%

detected by internal audit

ACFE 2026

1 in 5

inspected engagements lacking sufficient evidence

PCAOB

23%

of files had significant findings

CPAB

What inspection keeps finding: management review controls tested for existence, not precision · data feeding controls (IPE) taken on faith · one ITGC failure invalidating every dependent control · fraud-risk procedures that do not match the risk

Sources: ACFE, Occupational Fraud 2026: A Report to the Nations (14th ed.), 2,402 cases across 143 countries and territories. · PCAOB, 2024 Inspection Reports · Canadian Public Accountability Board, 2025 Annual Inspections Results

Canadian National Conference

RESILIENCE by Design

Three Ways A Function Can Be Built

FRAGILE

Breaks under stress and may not know it yet

ROBUST

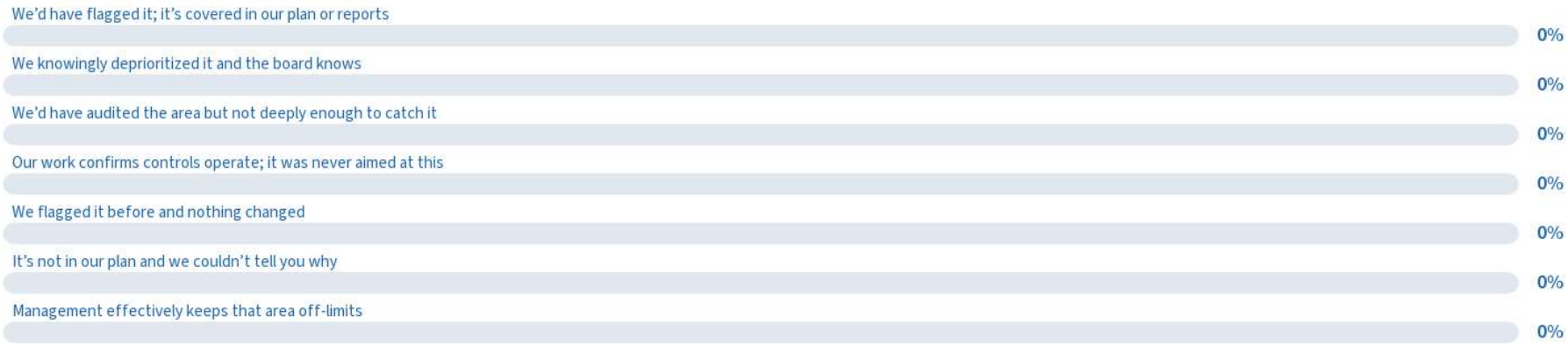
Survives stress unchanged; where most functions live

ANTIFRAGILE

Gets stronger because of stress; where this session aims

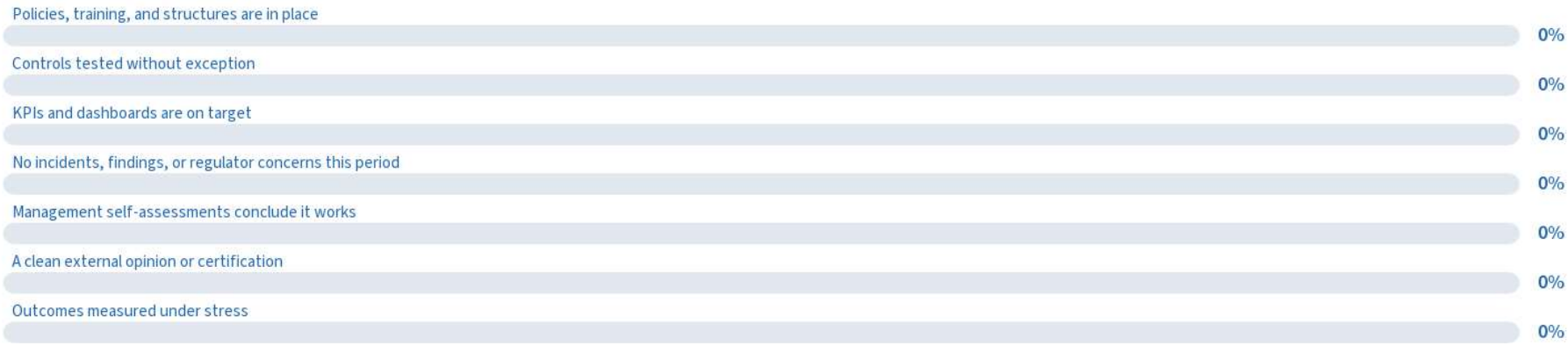
The next 50 minutes: a diagnostic for your function · a model to score against · a board page

If a significant control failure or fraud surfaced next quarter, which is closest to your honest expectation?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

How does your organization currently define program effectiveness?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

What “Effective” Actually Means

“The demonstrated ability to produce the intended outcome under real conditions, **including against the people motivated to defeat it,** evidenced to a standard that would survive hostile scrutiny.”

For an audit function, the intended outcome is: your assessment reflects reality; no material risk undiscovered, none inflated. A sober conclusion.

“Real conditions” means: the conditions your work actually meets, pressure, adversaries, incomplete information, not the conditions of a walkthrough.

→ *The six pressures — two slides from now.*

Canadian National Conference

RESILIENCE by Design

How Frameworks Define It

Source	How it defines “effective”
PCAOB — AS 2201 (your SOX opinion)	Reasonable assurance of reliable reporting, and if a material weakness exists, ICFR “cannot be considered effective.” Effective is defined by nothing found.
The IIA	Control is adequate if “planned and organized (designed) in a manner that provides reasonable assurance”, design sufficiency, plus conformance with the Standards.
ISO 9000 — inherited by every ISO management standard (37301, 45001, 27001…)	“Extent to which planned activities are realized and planned results achieved”, effectiveness graded against your own plan.
THIS SESSION	**The intended outcome, under real conditions, including against the people motivated to defeat it, evidenced to survive hostile scrutiny.**

None includes the adversary. None makes evidence part of the definition. None measures against reality rather than the plan. *That is the difference.*

RESILIENCE by Design

How To Assess Effectiveness



The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

Five Rungs of “It Works”

5	**ANTIFRAGILE**	Improves because of stress; this session aims here
4	**EFFECTIVE**	Produces the outcome under real conditions; regulators now ask here (FINTRAC effectiveness reviews)
3	**OPERATING**	Performed as designed, consistently; CSOX testing lives here
2	**DESIGNED**	Would work if performed as described; the walkthrough
1	**DOCUMENTED**	The artifact exists

What “Pressure” Means For An Audit Function

The pressure	The moment it arrives	The question it asks you
EVENT	A fraud, breach, or failure surfaces	*What did your program catch and what caught this instead?*
SCRUTINY	A regulator, inspector, monitor, or plaintiff reads your workpapers with hostile eyes	*Would your evidence survive?*
RESOURCE	The budget conversation arrives	*What does the plan shed first and who decided that?*
VELOCITY	The risk changes faster than the annual cycle	*Does your universe describe an organization that still exists?*
POLITICAL	Management leans on scope, access, or a rating	*What does it cost you to hold the line?*
HINDSIGHT	“Where was internal audit?” asked afterward, with full knowledge	*Was your answer aimed, deep enough and heard?*

Effectiveness is judged at these moments, not at year-end.
“Under real conditions” means under these.

Canadian National Conference

RESILIENCE by Design

The Ground Moved Under This Profession

WHY NOW

STANDARDS	**2024 Global Internal Audit Standards** — every standard now carries “evidence of conformance”; we now face what we asked of clients
MANDATES	**Mandatory Topical Requirements land mid-cycle:** Cybersecurity (Feb 2026) · Third-Party (Sept 2026) · Organizational Behavior (Dec 2026) — the rollover plan cannot absorb this
ENFORCEMENT	**Design ≠ performance, repeatedly proven** — SNC-Lavalin to TD Bank, the pattern is structure that looked mature on paper

Canadian National Conference

RESILIENCE by Design

Two Assurance Professions. Two Kinds of Scrutiny.

THE ASYMMETRY

EXTERNAL AUDIT	INTERNAL AUDIT
Inspected every year	Assessed once every five years
By an independent regulator, with hostile eyes	By a reviewer we select and pay
Results published, by firm name	Results private, often summarized to a paragraph
And improving because of it	**Often validating our own self-assessment**

You've seen what inspection finds.

So when our reports say "no significant issues", ***what would OUR rate be, if anyone were looking?***

Canadian National Conference

RESILIENCE by Design

Five Systems X Five Criteria

The systems are how a function is built. The criteria are how any system gets stronger, or weaker, under stress.

CRITERIA *the physics: how things break (after Taleb)*

SYSTEMS *the anatomy: what can be fragile*

	Skin in the Game Someone bears the cost of being wrong, and the credit for being right	**Optionality** Doors opened before they are needed; access stored, not requested	**Tinkering & Stressors** Small, deliberate stress applied; errors turned into method	**Concentration** No single channel, person or provider relied on unexamined	**Asymmetry** Reach where the downside lives; silence and suppression priced
The Mandate · Reach & standing What audit may examine, how far up it reaches, and whether it survives the pushback					
The Plan · Aim Whose inputs decide where audit looks, and whether every gap is priced to the board					
The Instrument · Capability The depth and expertise to challenge an expert, with evidence that survives inspection					
The Voice · Candor Whether findings are told straight and tracked to consequence, not left to age					
The Mirror · Self-correction Whether the examiner examines itself, and changes when it finds something					

25 cells · 56 questions · Yes = 3 · Partially = 2 · No = 1 → each system banded **Fragile · Robust · Antifragile**

Canadian National Conference

RESILIENCE by Design

RESILIENCE by Design

Application



The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

The Mandate: Reach

The Mandate is the function's authority: the permission structure that decides what audit may examine and how far up it may reach. Present and operating, these five properties build a mandate that strengthens under pressure; each one missing introduces a specific fragility, often silently.

Properties (Present, they build antifragility; missing, they introduce fragility)	The Antifragile Component
1. The charter grants unrestricted scope and practice matches it	**Optionality** — *every door already open*
▲ 2. Executive-owned and politically sensitive areas actually audited within two years	**Asymmetry** — *reach where the downside lives*
3. No inherited carve-outs ; every exclusion is a documented, current decision	**Concentration** — *no unexamined assurance monopolies*
4. Reliance on other assurance providers is assessed and reported	**Concentration** — *dependency made visible*
8. Unrestricted access to hotline, turnover, regulator, and override data	**Concentration** — *inputs management cannot shape*

▲ **Deal-breaker — absence alone renders the system fragile, and silently.** *Full criteria: your workbook, System 1. Read each property in the negative, imagine it absent, and this becomes the risk assessment.*

Canadian National Conference

RESILIENCE by Design

The Mandate: Standing

Reach is only half. These six properties govern standing: whether the CAE and the function can survive using the reach when someone pushes back.

	Properties — present, they build antifragility; missing, they introduce fragility	The antifragile component
▲	**5.** CAE appointment, evaluation, and compensation governed by the committee	**Skin in the Game** — *the right skin, installed*
	6. The CAE attends the full committee meeting, including executive sessions	**Asymmetry** — *presence, not summons*
	7. Standing presence at key management forums — observer, voice not vote	**Optionality** — *early sight, stored access*
▲	**9.** Restrictions reported to the board when they occur — and the board acts	**Asymmetry** — *suppression priced, never silent*
	10. An executive's career depends on how they answer findings, not on receiving them	**Skin in the Game** — *response, not receipt*
	11. The charter itself is reviewed with the committee on a defined cycle	**Tinkering** — *the mandate, maintained*

▲ **Deal-breaker — absence alone renders the system fragile, and silently.** *Full criteria: your workbook, System 1. Read each property in the negative, imagine it absent, and this becomes the risk assessment.*

Canadian National Conference

RESILIENCE by Design

The Mandate: Post-Mortem SNC Lavalin 2012

The audit that would have passed

Code of ethics	✓ in force
Agent-payment policies	✓ documented and approved
Board and committees	✓ established, meeting, minuted
CFO review of payments	✓ **operating and the control worked; he objected**

Illustrative reconstruction, from the public record.

The Mandate: Post-Mortem SNC Lavalin 2012

What was never asked

▲ №2 Could examination reach executive activity? The payments were authorized at the CEO's level, above every control that worked.

▲ №9 When the CFO's objection was overruled, twice, did anyone tell the board? The board learned from an investigation, not an escalation.

№8 Could anyone see inside a division not required to break out its projects to the board?

What it cost

$56M to agents whose identity was never established · the CEO's departure · police raids · class actions · a decade of consequence

"Can't govern something they don't know about." *— the board chair, afterward*

Canadian National Conference

PULSE 1 Your own function on THE MANDATE: **FRAGILE** · **ROBUST** · **ANTIFRAGILE**

RESILIENCE by Design

The Mirror: Self-Testing

The Mirror is the function's self-correction. Whether the examiner examines itself, and whether anything changes when it finds something. *These four properties govern self-testing; the stress a function applies to itself before the world applies its own.*

Properties — present, they build antifragility; missing, they introduce fragility	The antifragile component
1. The QAIP is alive and annual assessments that demonstrably change practice	**Tinkering & Stressors** — *self-applied stress*
▲ **2.** A missed risk triggers a formal post-mortem that changes the method	**Tinkering** — *errors metabolized, not filed*
3. External challenge between the five-year EQAs; peer review, red team	**Stressors** — *scrutiny imported on purpose*
▲ **4.** A sustained quiet period triggers examination of detection capability	**Asymmetry** — *silence is a question, not comfort*

▲ Deal-breaker: absence alone renders the system fragile, and silently.

Full criteria: your workbook, System 5. Read each property in the negative, imagine it absent, and this becomes the risk assessment.

Canadian National Conference

RESILIENCE by Design

The Mirror: Honest Measurement

Self-testing is only half. *These five properties govern whether the self-view can be trusted, independent, multi-sourced, and held to the same standard we apply to everyone else.*

Properties (Present, they build antifragility; missing, they introduce fragility)	The Antifragile Component
5. EQA results go to the board in full, with a tracked action plan	**Asymmetry** — *nothing softened in transit*
6. Performance measures include detection outcomes; misses matter	**Skin in the Game** — *being wrong costs something*
7. Quality assessment is independent of the work assessed	**Concentration** — *nobody grades their own homework*
8. Self-assessment uses data beyond the function's own records	**Concentration** — *outside measures, trusted more*
9. Our own evidence would survive the scrutiny we apply to auditees	**Skin in the Game** — *our standard, applied to us*

The Mirror Post-Mortem: SVB & Fed Reserve

WHAT ASSURANCE WOULD HAVE VERIFIED — AND PASSED

Supervision in place, on schedule ✓ · **Findings** identified, analyzed, escalated ✓
Governance rated deficient in 2022; the rating existed ✓ · **The file** complete ✓

WHAT WAS NEVER ASKED IN TIME

- **№2** when supervision missed, what changed — and at what speed relative to the risk?
- **№8** did the quiet years trigger examination of detection capability itself?
- **№5** did misses cost anyone anything, before the collapse made them cost everyone everything?

THE OUTCOME AND THE TURN

The bank failed within a year of the deficient rating · then the Federal Reserve reviewed its own supervision, publicly, and named its own failures

The Mirror, working at the cost of needing it too late. Your Barr report gets written either way: by you now, or about you later.

One Measurement, Three Zoom Levels

The frame, the ladder, and the tool are the same system

The frame (you pulsed it)	The ladder (you climbed it)	The evidence (you'll report it)
FRAGILE	**Rungs 1–2** Documented · Designed	Paper exists; nobody has watched it work
ROBUST	**Rung 3** Operating	Controls performed as designed; where most functions live, and where most reports stop
ANTIFRAGILE	**Rungs 4–5** Effective · Improving	Outcomes under real conditions; proven by six measurable indicators (defined in next section), not claimed

*The bands you pulsed, the rungs you climbed, and the KPIs you will report to the board are **one measurement at three zoom levels.***

RESILIENCE by Design

Board Reporting



The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

Proving It

The report we all send — and it conforms

Annual plan: 87% complete	✓ *9.4 · plan and progress, communicated*
43 findings closed this quarter	✓ *11.3 · results, communicated*
Utilization and budget: on target	✓ *10.1–10.2 · resources, communicated*
Team training hours: delivered	✓ *10.2 · competencies, maintained*
Performance measures: green	✓ *12.2 · methodology exists — measures self-chosen*
External quality assessment: generally conforms	✓ *8.4 · …five years ago*

Every required communication, present. Fully conformant. ***And none of it answers the question the committee is holding: can we rely on this?***

Canadian National Conference

RESILIENCE by Design

Eight Sections: What Each Is & How You Build It

THE EFFECTIVENESS REPORT · SECTIONS 1–4

Section	What it is	Source data · how it's built
1 Fragility profile	The function's own 5×5 self-assessment, honestly banded, including anything rated Fragile	*Completed workbook (all 25 cells) · average Yes/Partially/No = 3/2/1 per system; band by cutoffs*
2 Escalation outcomes	Findings raised, their aging, and what happened, incl. risk formally accepted instead of remediated (11.5)	*Findings tracker + AC minutes · % of past-due significant findings escalated or formally accepted; aging in days*
3 Competence disclosure	The areas we cannot yet opine on with authority, named, each with its remediation (co-source, training, deferral)	*Competence map vs. the plan · count of plan areas with no credible internal challenge; the fix named for each*
4 Coverage vs. enterprise risk	Every top ERM risk: covered · relied on (and assessed) · or deferred with the exposure priced	*ERM register vs. plan + assurance map · each top risk tagged one of three ways; deferrals priced in words*

Eight Sections: What Each Is & How You Build It

THE EFFECTIVENESS REPORT · SECTIONS 5–8

Section	What it is	Source data · how it's built
5 Effectiveness KPIs	Six numbers measuring the function's own exposure Defined next slide: K1–K5 trending quarterly, K6 annually	*Records you already hold · six formulas on next slide*
6 Plan adaptation	What moved mid-year, what triggered it, what was retired — the plan as a living instrument	*Plan-change log + re-earn session output · adds with triggers; retirements with rationale; reserve % remaining*
7 Governance & incentives	How the function itself is governed and what consequences attach to doing assurance well or badly	*AC charter + CAE evaluation criteria · current stage*
8 Value in five forms	Assurance · protection · improvement · enablement · foresight with the honest caveat: the biggest value, losses that never happened, cannot be counted	*Findings ledger + measures scan + advisory log · countable items per form; the caveat in one sentence*

The KPIs

Six numbers that measure the function's own exposure · K1–K3

KPI	Definition	What it exposes	Reading it
K1 · Coverage-to-consequence ratio	% of audit hours on top-decile-consequence risks read WITH K2: the ranking is only as honest as the inputs	*Effort mapped to feasibility, not consequence*	**Fragile:** coverage follows ease **Antifragile:** reallocation visibly follows risk
K2 · Input concentration index	% of planning inputs from management-shaped channels (workbook carries the channel taxonomy)	*Capture of the plan's intelligence*	**Fragile:** one curated channel **Antifragile:** independent streams grow yearly
K3 · Draft-to-final delta	Rating movement between draft and final, and its direction	*Softening under relationship pressure, the kind that happens late; this measure cannot see softening that happens before the draft is written*	**Fragile:** one-way drift **Antifragile:** movement both ways and examined

*K1–K5 measure the conditions: aim, independence, candor, consequence, currency. K6 measures the **RESULT**. All from records you already hold. More in the workbook: time-to-escalation, post-mortem completion, reserve deployment.*

Canadian National Conference

RESILIENCE by Design

The KPIs

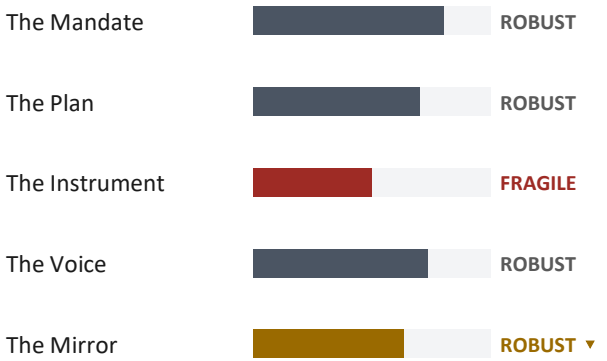
Six numbers that measure the function's own exposure · K4–K6

KPI	Definition	What it exposes	Reading it
K4 · Findings-to-consequence rate	% of past-due significant findings escalated or formally accepted (11.5)	*Consequence-free assurance*	**Fragile:** findings age silently **Antifragile:** 100%: nothing ages in silence
K5 · Universe currency delta	Material items in org records absent from the audit universe; an annual trend, not a quarterly pulse	*The risks that cannot be ranked*	**Fragile:** the map lags the territory **Antifragile:** trending to zero
K6 · Detection ratio: the outside measure	Of significant issues surfaced this year, incidents, hotline, regulator, external, the share internal audit had already identified or flagged. Annual, with narrative	*Whether the function actually detects what matters: the outcome, not the conditions*	**Fragile:** the outside world finds it first **Antifragile:** audit was already there the ACFE statistic, computed for your own shop

INTERNAL AUDIT EFFECTIVENESS — AUDIT COMMITTEE DASHBOARD – Illustration Only

Eight sections · illustrative model

1 · FRAGILITY PROFILE — the function, self-assessed



Scale 1.0–3.0 · one system honestly Fragile — its remediation is section 3, not a secret

5 · EFFECTIVENESS KPIs

K1 · Coverage-to-consequence

68%

of hours on top-decile risks

▲ from 54%

K2 · Input concentration

41%

of plan inputs management-shaped

▼ from 63%

K3 · Draft-to-final delta

4 of 11

ratings moved — all downward

■ AMBER · under review

K4 · Findings-to-consequence

87%

past-due significants escalated or accepted

▲ · 1 risk accepted (11.5)

K5 · Universe currency

6 items

absent from the universe — 1 significant (a newly acquired operation) · 5 limited exposure

■ significant gap closes next cycle

K6 · DETECTION RATIO

3 of 5

significant issues that surfaced this year, audit had already flagged

THE OUTSIDE MEASURE · annual

4 · COVERAGE VS ENTERPRISE RISK

14 top risks: 11 covered · 1 relied on (and assessed) · 2 deferred — exposure priced, before the board

6 · PLAN ADAPTATION

3 audits added mid-year (defined triggers) · 2 retired via the re-earn test · reserve remaining: 6%

7 · GOVERNANCE & INCENTIVES

CAE evaluation & compensation: committee-governed ✓ · detection outcomes in evaluation: partial ▲ · recognition for issues surfaced: in place ✓

2 · ESCALATION & CONSEQUENCE — nothing ages in silence

All past-due significant findings escalated or formally accepted — none pending silently · 1 risk accepted by management (privileged access reviews, 94 days) — before this committee under Standard 11.5 · 1 repeat finding: rating raised, root cause escalated — not re-issued

3 · COMPETENCE DISCLOSURE 8 · VALUE

Two areas where we currently lack the expertise to challenge management: AI model risk — specialist co-source engaged · climate reporting methodology — training underway, complete Q4. Until then, “no findings” in these areas carries less assurance.

Value — countable floor: $2.1M recovered or prevented. The biggest value — losses that never happened — cannot be counted.

Every figure computes from records the function already holds · K1–K5 quarterly, K6 annual · Adopt in stages — do not walk this into a cold committee whole · ILLUSTRATIVE — fictional data

Why This Works In Plain Terms

KPIs make problems visible. Five numbers make the function's own weaknesses show up, in figures, every quarter.

Incentives make visibility matter. When the numbers are bad, someone's evaluation changes, so they get acted on, not filed.

> Together they form a loop: the function is forced to see what goes wrong, and forced to respond, so it comes out of each stress stronger. **That is antifragility, a mechanism, not a metaphor.**

It meets our definition of effective, piece by piece:

- **DEMONSTRATED** — numbers, not assertions.
- **AGAINST THE ADVERSARY** — K2–K4 catch steered inputs, softened ratings, ignored findings.
- **SURVIVES SCRUTINY** — a number you can show again next quarter.

You chair the audit committee receiving this report. Which section would most convince you that you can rely on this audit function?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

This Month, One Move

Run the assessment.

- Fifty-six questions · records you already hold · **one afternoon**
- Your profile tells you where to respond; start at the **anchor cells of your weakest system**
- Your **Poll 3** answer already told you where that probably is

Canadian National Conference

RESILIENCE by Design

If a failure surfaced tomorrow, could you show, with evidence, **that your function was aimed at it, looked hard enough, and was heard?**

Canadian National Conference

RESILIENCE by Design

RESILIENCE by Design

Questions



The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

Thank you.

Lori Caltagirone, CPA

President, Sunesis

lcaltagirone@sunesiscorp.com

Katrina Mamuric, CPA

Director, Client Service and Business Development

kmamuric@sunesiscorp.com



The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

https://www.sunesiscorp.com/

RESILIENCE by Design