SECURANCE CONSULTING
Advantage of Insight | AI

AUDIT BY RISK, NOT ROTATION

Why Local Government Internal Audit Needs a Multi-Year, Risk-Based IT Audit Plan — and How to Build One That Survives Committee Scrutiny

CONTENTS

Executive Summary

A local government internal audit function always has more technology to examine than it has hours to examine it. The financial ERP, the identity platform that governs who can touch what, public safety systems, the network, and the dozens of applications layered on top are all plausibly in scope, and no team can reach them all in a single year. Every IT audit plan is, at its core, a decision about where to concentrate a scarce resource. The real question is whether that decision is made deliberately, on the evidence of risk, or by default, on the force of habit.

Most IT audit plans are made by habit. They rotate through systems on a familiar cadence and present that rotation to the audit committee as coverage. It looks orderly, but it optimizes for the wrong thing — giving every system its eventual turn rather than directing audit effort to where the organization's exposure and consequences are greatest. Asked why a particular set of systems was chosen for a particular year, rotation offers no rationale beyond seniority in the queue.

A multi-year, risk-based IT audit plan answers that question with a defensible rationale. It ranks the full technology estate by composite risk — weighing not just the threat a system faces but how much the organization relies on it, what its failure would cost, how complex it is to administer, and how recently it changed — then sequences coverage across a defined cycle so the highest-consequence systems come first, with a documented record of what was considered and set aside.

It is neither a forecast locked in place nor a plan rebuilt from scratch every year. It is a roadmap: a sequence the organization commits to and follows, adjusting only when a material change genuinely warrants it. For a small, stretched internal audit function, that combination — prioritized, complete, and stable enough to execute — is what makes coverage both achievable and defensible.

Every IT audit plan is a decision about where to concentrate a scarce resource.

The Prioritization Problem at the Heart of IT Audit

Every internal audit shop knows, in the abstract, that it cannot audit everything. Few construct their plans around that limitation, even though it is the very problem a plan needs to solve. A midsized local government may run scores of distinct auditable technologies while its internal audit team numbers only a handful of people, not all of them technology specialists. In any given year, that team can examine a fraction of the estate in real depth. What it chooses to examine immediately, and what it leaves for later, is the most consequential judgment in the entire plan.

Rotation is the most common way that judgment gets made, and the appeal is easy to see. Maintain a list of systems, give each one its turn every few years, and send whatever was audited most recently to the back of the line. The approach is simple to explain and hard to dispute because it rests on a principle everyone accepts: fairness. Every system gets attention eventually.

But fairness to systems is not the same as protection for the organization, and the two often point in different directions. Rotation treats the time elapsed since the last audit as the trigger for the next one — as though elapsed time, not risk, were the measure of where attention should be directed. It places a low-stakes records-retention application on the same conveyor belt as the financial ERP that processes the county's transactions, or the identity platform that controls access to every system — each entitled to the same slot regardless of how much more rides on it. The result can satisfy a procedural definition of coverage while leaving the organization's most consequential systems examined no more often than its least consequential ones.

Rotation Fails Because Risk Concentrates — and Not Only Where Attackers Do

The case against rotation isn't that it is unfair; it's that it ignores where risk gathers. And risk gathers unevenly along several dimensions at once — not just the one that makes headlines.

The headline dimension is security exposure. According to Verizon's 2026 *Data Breach Investigations Report*, exploitation of unpatched vulnerabilities has become the single most common way attackers gain their initial foothold. This is the first time in the report's history that vulnerability exploitation has overtaken stolen credentials as the most common initial access vector. And third-party involvement now appears in nearly half of all breaches.[1] Security risk doesn't distribute itself evenly; it concentrates in a handful of identifiable, auditable areas: patch and vulnerability management, third-party and vendor oversight, identity and access, and the systems that depend on them.

Even known weaknesses linger where no one is looking. Only about a quarter of the critical vulnerabilities on CISA's Known Exploited Vulnerabilities list were fully remediated in 2025.[2] While the percentage of remediated vulnerabilities declined, the median time to patch rose from 32 to 43 days.[3] For an auditor, a gap like that is a signal; it marks where assurance is most needed.

WHERE SECURITY RISK CONCENTRATES

31%

of breaches begin with exploitation of an unpatched vulnerability — now the leading initial access vector

48%

of breaches involve a third party — a 60% jump in a single year

26%

of critical CISA KEV vulnerabilities fully remediated in 2025, down from 38%

But security is one axis, and a plan built on it alone is still a single-axis plan. Risk concentrates just as unevenly along dimensions that have nothing to do with an attacker. Financial exposure gathers in the system that moves the most money — the ERP that processes payroll and payments, where the dominant risk may be error or fraud, not intrusion. Operational reliance gathers in the platforms whose failure halts services — computer-aided dispatch, utility SCADA, permitting — where availability, not confidentiality, is the exposure. Control risk gathers in the systems that recently underwent a major migration, or that only one soon-to-retire administrator fully understands. None of these are breach stories. All are risks a defensible plan must weigh.

RISK CONCENTRATES ALONG FOUR AXES

01 Security exposure

Patch and vulnerability management, third-party oversight, identity and access — and the systems that depend on them.

02 Financial exposure

The systems that move the most money, where the dominant risk may be error or fraud, not intrusion.

03 Operational reliance

Platforms whose failure halts services — dispatch, utility SCADA, permitting — where availability is the exposure.

04 Control risk

Systems that recently underwent a major migration, or that only one soon-to-retire administrator fully understands.

That is exactly what rotation is structurally blind to and what a composite risk assessment is built to surface. Consider a concrete case. A rotation schedule audits the financial ERP whenever its turn comes up. Rank instead by the risk that tends to dominate informal judgment — the threat of attack — and the ERP might land mid-pack: it is not the most internet-exposed system in the estate. Few shops would say they rank on security alone, but in the absence of a structured method it is the dimension that crowds out the others, because it is the one in the headlines.

Score the ERP across every dimension, though — the organization's near-total reliance on it, the financial consequences of its failure, the volume of privileged access it requires, a recent version upgrade — and it rises to the top on the strength of factors a breach statistic never captures. The system that most needs auditing is not always the one most likely to be attacked. Composite scoring is what tells them apart; single-axis thinking, whether the axis is rotation or security threat, cannot.

Rotation gives your highest risks no more attention than your lowest — and a security-only plan misses the risks that aren't about security at all.

The stakes of misdirected attention are real in every direction. A breach is one form of costly failure: IBM's *Cost of a Data Breach 2025* put the U.S. average at a record $10.22 million and the public sector average at $2.86 million.[4] But an ERP failure that suspends payroll, a botched migration that corrupts records, or an outage that halts permitting carries its own price in diverted budgets, disrupted services, and eroded public trust — costs that never appear in a breach report. When audit capacity is finite, every hour spent examining a low-risk system on the strength of its place in the rotation is an hour not spent where a finding might have prevented a loss of any of these kinds.

ONE FORM OF COSTLY FAILURE

$10.22M	$2.86M
U.S. average cost of a data breach — a record high	Public sector average

The Resource Reality of Local Government

If risk concentration is the reason to prioritize, resource scarcity is the reason prioritization is not optional. Local governments cannot close the gap between what needs auditing and the hours they have to audit it simply by doing more; the people and money to do more are precisely what they lack.

The staffing picture is well documented across the internal audit profession. The IIA's *Pulse of Internal Audit*, which surveys chief audit executives across North America, found budget cuts rising sharply between 2024 and 2025 while the share reporting budget increases fell. Staff reductions rose over the same period, and about half of CAEs now describe their functions as underfunded even as their scope grows.[5] The gap is not only headcount but expertise: more than four in 10 reported lacking the skill sets their work now demands, with cybersecurity and IT among the most cited areas of deficiency.[6]

IIA, Pulse of Internal Audit.

Local government sits at the sharp end of these averages. In the *Pulse's* public sector segment, IT and cybersecurity accounted for only 16 percent of audit effort. But the report skews toward larger federal, state, and big-city functions. County and municipal shops are typically smaller, often three to eight auditors with limited or no IT audit specialization on staff. Even in the *Pulse's* own data, public sector functions at organizations of 5,000 or fewer employees average just 7.2 full-time auditors — that is the whole shop, covering the entire audit universe, not just the IT portion of it.[7] That is precisely the profile least able to spread scarce, specialized hours across a growing estate without a method for deciding where they go first.

None of this argues for lowering expectations. It argues for using scarce capacity purposefully. Scarcity is the condition under which prioritization pays the highest return: when audit hours are abundant, the order in which they are spent hardly matters; when they are severely limited, that order becomes one of the most important factors in whether the plan protects the organization. A risk-based plan is not a luxury for well-funded shops. It is the discipline that lets a small team direct its limited hours to the systems where a finding matters most.

The Case for the Long View

If the technology environment changes continuously, doesn't a multi-year plan risk being out of date before reaching the end of its term? The question deserves a direct answer, because the answer is the crux of the approach.

A well-built multi-year plan does not assume the world will hold still, nor does the team rebuild it from scratch each year. What keeps it sound is not constant rescoring but disciplined adaptability. The plan can be followed with confidence, and the sequence is adjusted only when warranted by a substantial internal or external change, such as a major system migration, a significant new regulatory obligation, a serious incident, or the arrival of a consequential new system. Absent such a trigger, the plan stands and the team gets on with executing it. A three-year horizon is stable enough to anchor a full cycle of audit work, yet responsive enough to stay relevant when circumstances truly change. At the close of each cycle, the plan is rebuilt from a fresh risk assessment, so each new cycle reflects the organization's current risk picture.

A multi-year plan is neither a fixed mandate nor a moving target; it directs the work until a substantial change calls for revision.

Set against that, the usual alternatives — planning one year at a time, or auditing reactively as issues surface — are not meaningfully more current, but they are far less complete. Reactive, year-by-year auditing chases whatever is loudest: the most recent incident, the newest system, the concern raised most forcefully in a meeting. It offers no assurance that the full estate is covered on any defined timeline, and it makes blind spots the norm. A multi-year plan is the only structure that can guarantee every system is addressed within a bounded, defensible period, while ensuring those representing the highest risks are addressed first.

Beyond completeness, a multi-year horizon delivers three things an annual view cannot. First, it enables resource and skills planning: knowing a specialized systems audit is scheduled for next year lets a resource-constrained government arrange co-sourcing, outsourcing, or training in advance rather than scrambling. Second, it provides continuity through the staff turnover inevitable in a small function, so the plan survives the departure of the person who built it. And third, it creates a defensible record — a documented, risk-ranked sequence the audit leader can put in front of an audit committee, an external auditor, or a post-incident reviewer and defend on its merits.

There is a governance dimension as well. Audit committees and governing boards are increasingly expected to show they oversee technology risk deliberately rather than anecdotally — the same expectation embodied in enterprise control frameworks such as COSO, where risk assessment is a foundational component. A multi-year, risk-ranked plan is the ideal artifact to meet it. It turns "we audit our systems periodically" into "here is our risk-ranked coverage plan, here is why it runs in this order, and here is what would cause us to change it." That is the difference between an assurance the board hopes is true and one it can see.

What the standards say

Risk-based, prioritized IT audit planning is not a preference — it is what the profession's standards require, and what the broader control frameworks are built around.

STANDARDS THAT REQUIRE RISK-BASED AUDIT PLANNING

IIA Global Internal Audit Standards. The standards that govern the internal audit profession explicitly require the audit plan to be built on a documented assessment of risk. For an internal auditor, risk-based planning isn't best practice — it's the mandate. [8]

ISACA IT Audit Framework. The professional standards for IT auditing likewise require engagements and plans to be driven by a risk assessment, sequencing work by where risk to the organization's objectives is greatest. [9]

FRAMEWORKS WHOSE OWN LOGIC IS RISK-PRIORITIZED

COBIT. Links IT processes to enterprise goals, so audit effort can be weighted toward the areas where failure would most threaten objectives. [10]

ISO/IEC 27001. Frames security around risk treatment, so coverage can be sequenced by residual risk rather than uniform, control-by-control review. [11]

NIST Cybersecurity Framework. Profiles current versus target posture across cybersecurity objectives, surfacing the widest capability gaps to address first. [12]

NIST Risk Management Framework (SP 800-37). A government-oriented framework built entirely around categorizing systems by risk and prioritizing accordingly — the same logic, applied to system authorization. [13]

Read together: direct audit effort by risk, and revisit priorities when the risk profile changes.

The Anatomy of a Risk-Based Audit Plan

Agreeing that a plan should be based on risk is the easy part. Building one that genuinely is — and that withstands a committee chair's questions — takes a specific, repeatable method.

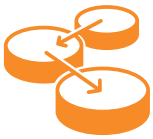
1. Build a complete, current IT audit universe. Before anything can be ranked, the field has to be defined — not as broad functional areas ("the network") but as the specific, auditable technologies and processes that make up the environment: enterprise applications, infrastructure components, identity and access management tools, public safety systems, operational technologies, and the IT processes that support them. In a typical local government, this runs to dozens of discrete entries.

2. Score each technology and process across the dimensions that matter to the organization. Start with the dimensions themselves. Reliance, operational impact, financial exposure, security threat, and recent major change are a workable starting set, though the right list is particular to the environment being scored.

The most reliable ratings come from the people who run the environment. Interview the IT staff and business process owners who administer each technology and process, and ask them to rate what they own across every dimension. Aggregated, those ratings produce a composite score grounded in the environment, rather than in the audit team's impression of it. A single axis cannot do that work because threat and consequence are independent. The system most likely to fail and the system whose failure would cost the most are rarely the same one.

EXAMPLES OF DIMENSIONS. YOURS MAY DIFFER

01 **Reliance on the technology**	02 **Complexity of the technology**	03 **Degree of customization**
04 **Adequacy of administering staff**	05 **Operational impact if it fails**	06 **Financial exposure**
07 **Security threat faced**	08 **Administrative burden**	09 **Recent major change**



3. Sequence the work across a multi-year cycle, highest risk first. With composite scores in hand, the sequence follows. The systems that present the most risk to the organization come first. Those are not necessarily the systems most likely to fail, but the ones whose failure or compromise would cost the organization the most, whether in disrupted services, financial loss, or compliance penalties. The plan then works down the ranked list across a defined horizon. Three years is the horizon Securance recommends: long enough to demonstrate complete, deliberate coverage and short enough that the ranking stays meaningful across its life.

What the deliverable looks like — a one-page plan (illustrative, from a redacted engagement)

TECHNOLOGY / PROCESS	COMPOSITE SCORE	RISK TIER	AUDIT YEAR
Patch Management	**39**	HIGH	Year 1
Disaster Recovery Planning	**38**	HIGH	Year 1
Accela (Permitting)	**36**	HIGH	Year 1
Change Management	**36**	HIGH	Year 2
Firewall / Router / Switch	**36**	HIGH	Year 2
NorthStar (Financials)	**35**	HIGH	Year 2
Database Security	**34**	MEDIUM	Year 3
Vendor Management	**33**	MEDIUM	Year 3

Note what rose to the top: the two highest-risk items are IT processes, not the systems an attacker would target first. That is composite scoring at work — reliance, recoverability, and control maturity outweighing raw threat.

4. Maintain the plan, and only revise it following a major change. The team follows the sequence with confidence and revisits the ranking only when a significant change — a major migration, a new regulatory mandate, or a serious incident — calls for it. At the close of the cycle, a fresh risk assessment resets the sequence for the next one.

5. Document what was excluded, and why. The step most plans skip is the one audit committees most appreciate: recording the technologies that were evaluated and deliberately set aside, with the reasoning for each. Committees ask about the systems that are not on the plan; a plan that has already answered that question in writing turns its most exposed flank into evidence of rigor.

6. Translate the plan into a one-page view the committee can act on. The risk assessment behind the plan is a substantial document that includes methodology, scoring rubric, risk categories, the full inventory of technologies and processes, and the risk matrices that support the ranking. The plan itself is one page: the ranked technologies, their composite scores and tiers, and the year each is scheduled, in language a committee chair can absorb in minutes. The report underneath earns the plan its authority; the one page earns its approval.

Together these steps produce a plan with the property rotation and reactive auditing both lack: it is defensible in every direction. Each system on the plan is justified by its score; each system left off is explained; the sequence is driven by evidence; and the plan is maintained deliberately. When someone asks why these systems, in this order, the plan answers for itself.

DEFENSIBLE IN EVERY DIRECTION

Every system on the plan Justified by its composite score.	**Every system left off** Explained, in writing, before the question is asked.
The sequence Driven by evidence rather than by habit.	**The plan itself** Maintained deliberately, revised only when change warrants it.

Conclusion: Build the Plan That Holds Up

The argument comes down to a few durable facts. Audit capacity is finite, and especially so in local government. Risk is concentrated rather than evenly spread — and it concentrates along several dimensions, only one of which is the threat of attack. The cost of leaving the wrong system unexamined is significant, whether that cost arrives as a breach, a failure, a compliance violation, or fraud. And the profession's own standards already require audit effort to be directed by risk. Rotation addresses none of this; a risk-ranked, multi-year plan addresses all of it.

For a local government, the payoff is concrete. A plan built on composite risk scoring, sequenced across a defensible multi-year cycle, maintained as a stable roadmap, and documented down to what was deliberately excluded does more than satisfy an auditor. It puts scarce hours where they protect the most, it answers the committee's hardest questions before they are asked, and it shows residents and elected officials that technology risk is being managed by design rather than by default.

Audit plans also have a season. For many local governments, FY27 planning windows open in the fall, with the planning work — and any co-sourced audit support — typically scoped over the preceding summer. The organizations that enter the next cycle with a defensible plan are the ones building it now.

WHERE TO START: THE SIX STEPS

01	Build a complete, current audit universe of technologies and processes.
02	Score each technology across multiple risk dimensions.
03	Sequence the work highest-risk-first across a three-year cycle.
04	Maintain the plan; adjust only when a material change warrants it.
05	Document what you evaluated and deliberately excluded, with reasons.
06	Translate it into a one-page IT audit plan your committee can act on.

How Securance Can Help

A method is only as good as the expertise behind it. Judging which of dozens of technologies deserves the highest composite score means understanding how each system fails — not only how it might be attacked, but how it might break, be defrauded, or simply be too complex to control. That is as much a security and operations discipline as an audit one, and it is the expertise that budget and hiring pressures put out of reach for most local government audit teams.

Securance's IT audit planning service is built to close that gap. It rests on three pillars. The first is a risk-aligned, multi-category scoring methodology: every plan begins with a risk assessment scored across the dimensions the organization selects or defines for itself, so the ranking reflects that environment rather than a default. The second is an audit-committee-ready output: each in-scope technology receives a composite risk ranking that fixes its place in a multi-year sequence, delivered as a one-page view a committee chair can read in minutes. The third is senior-led delivery: the senior consultants who scope the engagement are the same ones who conduct the stakeholder interviews, make the scoring judgments, and build the plan.

The result is the plan described here: a complete universe of auditable technologies, each scored across the organization's own risk categories; a risk-ranked, multi-year sequence; a documented log of what was considered and excluded; and a one-page summary that answers the committee's most consequential questions before they're asked.

Two ways to see it for yourself, no obligation:

Download a redacted plan from an actual local government engagement — the full methodology, the scored register, and the one-pager containing a risk-ranked, multi-year audit sequence. It's free, and no call is required.

READ A REAL ONE

Book a consultation and we'll review your current or draft FY27 IT audit plan and show you where it's exposed to committee scrutiny — a working session on your environment, not a pitch.

GET A SENIOR READ ON YOURS

If your IT audit plan runs on rotation rather than risk, or you're not certain it would survive committee scrutiny, that's exactly the gap we close.

To learn more, visit: **www.securanceconsulting.com/services/it-audit-plan-development**

Sources

1. Verizon, 2026 Data Breach Investigations Report
2. Verizon, 2026 Data Breach Investigations Report
3. Verizon, 2026 Data Breach Investigations Report
4. IBM, Cost of a Data Breach Report (2025)
5. Institute of Internal Auditors (IIA), Pulse of Internal Audit
6. Institute of Internal Auditors (IIA), Vision 2035
7. Institute of Internal Auditors (IIA), Pulse of Internal Audit
8. IIA Global Internal Audit Standards (2024)
9. Information Systems Audit and Control Association (ISACA), IT Audit Framework (ITAF)
10. ISACA, COBIT
11. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001
12. National Institute of Standards and Technology (NIST), Cybersecurity Framework 2.0
13. NIST, Risk Management Framework, SP 800-37, Rev.2

Audit by Risk, Not Rotation

SECURANCE CONSULTING

Advantage of Insight AI

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com