The Last Mile of Assurance

Closing Findings Before They Become Failures

InConsult
risk advisory | audit | assurance

GuardianERM

Contents

Executive Summary

Assurance reports - whether from internal audits, external audits, penetration tests, vulnerability scans, root-cause analyses, or business continuity exercises, serve as important early warning systems for organisations. They can highlight critical, high impact risks and vulnerabilities in the control environment.

But their real value is only realised when the identified weaknesses are effectively actioned, implemented and closed i.e. remediated.

Too often however, actions from recommendations remain open for far too long or are closed superficially ("paper closures"), leaving organisations vulnerable to serious operational, financial, or reputational risks.

In many organisations, 30 - 40% of audit findings remain open for over 12 months.

Strong effective remediation governance remains one of the most cost-effective ways for boards, audit committees, and executives to materially reduce known risks.

This ebook explores why many organisations struggle with remediation, the potential consequences of delays or inaction, and outlines a pragmatic, repeatable framework to manage and validate actions.

Drawing on high-profile failures like Barings Bank, Equifax, and Carillion, it highlights the cost of delayed or inadequate follow-through of audit recommendations.

We propose a governance model that ensures both ownership and independent validation, supported by metrics, technology, and an implementation roadmap for success.

Why Assurance Reports Matter

Effective governance relies on a continuous flow of assurance artefacts and reports - independent, objective information that informs key stakeholders whether controls are working, risks are managed effectively, and obligations are met. Assurance reports play a foundational role in modern day governance.

Assurance reports come in many forms, each designed to examine specific risks, controls, and organisational capabilities. While the scope and methodology of each review and report differ, they all share a common purpose - to provide independent insight that strengthens governance, improves decision-making, and protects the organisation from financial, operational, cybersecurity, regulatory, and reputational risks.

The table below summarises the main types of assurance reports and their primary assurance focus, providing a clear view of how each contributes to a robust assurance ecosystem.

Assurance Report	Assurance Focus Area
Internal Audit Report	Effectiveness of internal controls, risk management processes, compliance with policies, and operational efficiency.
External Audit (Financial Statement Audit)	Accuracy and integrity of financial statements, financial reporting controls, and compliance with accounting standards.
Regulatory Review / Tripartite Review / Compliance Audit	Level of adherence to specific laws, regulations, prudential standards, licences, industry codes, and mandatory obligations.
Cybersecurity Assessment	Cybersecurity controls, maturity of cyber processes and culture, gaps in detection/response capability.
Penetration Test (“Pen Test”)	Assess the ability of systems to withstand simulated cyberattacks; exploitable vulnerabilities.
Vulnerability Scan	System weaknesses, outdated software, misconfigurations, and known security vulnerabilities.
Risk Management Framework Review	Evaluate maturity of risk governance, effectiveness of risk processes, alignment with standards and regulatory expectations.
Governance Review	Board and committee effectiveness, decision-making processes, reporting quality, and oversight arrangements.
ESG / Sustainability Assurance	Accuracy and completeness of ESG disclosures, sustainability reporting controls, and environmental/social governance practices.

Fraud & Corruption Review	Exposure to fraud risks, strength of anti-fraud controls, culture, and detection mechanisms.
Work Health & Safety (WHS) Audit	Safety controls, incident management, compliance with WHS legislation, and workplace risk exposures.
Engineering / Technical Inspection	Condition, integrity, safety, and performance of physical assets, infrastructure, or engineered systems.
Data Quality / Data Governance Audit	Accuracy, completeness, reliability, and governance of critical datasets and information assets.
IT General Controls (ITGC) Audit	Logical access, change management, IT operations, backup and recovery, and system governance.
Business Continuity Exercise / Review	Readiness to respond to disruptions, recovery capability, crisis management, and continuity planning.

Individually, each assurance report offers specific and valuable insights, but collectively, they are part of a critical early-warning system for the organisation. Across all the focus areas, assurance reports:

- Highlight issues that could lead to financial loss, compliance failures, or reputational damage.
- Provide independent evidence of weaknesses for boards, audit committees, and executives.
- Support informed decision-making and resource allocation for control improvement.
- Demonstrate accountability to regulators, auditors, insurers, shareholders and the community.
- Strengthen organisational resilience by driving continuous improvement.

When findings, recommendations and actions are not captured, tracked, and closed in a timely manner, the value of these assurance activities is lost, and risks can compound unnoticed. Conversely, when recommendations are captured, owned, and monitored through a structured system, assurance becomes a powerful driver of performance, trust, and risk maturity.

Boards, audit committees, and regulators increasingly expect organisations not only to identify issues, but to demonstrate credible, timely remediation supported by evidence.

So What? The real value of assurance reports is achieved only when insights are converted into actions, and actions are verified as effective. Closing the loop is not administrative – it is fundamental to resilience, governance integrity, and organisational trust.

Why Tracking Actions Matters

Identifying gaps, weaknesses, and control failures via an audit or assurance report is only the first step. Assurance activities - whether internal audits, external audits, penetration tests, or compliance reviews - deliver insight, not outcomes. Real improvement only occurs when organisations proactively and systematically track the remediation actions that flow from these reports.

Robust action tracking of remediations reduces the likelihood of repeat findings, minimises risk exposure, and provides a clear line of sight to assurance owners, executives, and regulators. It strengthens compliance with legislative and regulatory requirements, supports effective risk management, and demonstrates that the organisation takes its obligations seriously. For boards and audit & risk committees, timely and transparent remediation gives confidence that key risks are being addressed, not ignored or allowed to re-emerge.

When this discipline is missing, organisations frequently experience long-tail backlogs, unclear or shifting ownership, poor-quality updates, and inconsistent or incomplete evidence to support closure. These gaps not only undermine the credibility of the assurance program but also leave the organisation exposed to avoidable incidents, regulatory scrutiny, reputational damage, and wasted assurance effort.

Once again, tracking remediation is not administrative - it is a core governance discipline. It ensures that weaknesses identified across audits, cyber reviews, pen tests, BCP exercises, risk assessments, and other assurance activities are addressed, not merely acknowledged.

Barings Bank (1995)

Barings collapsed after a rogue trader in Singapore engaged in unauthorised trades, hiding mounting losses in secret accounts. Prior to the collapse, an internal audit conducted in 1994 had pointed directly to many of the weaknesses in both the risk management structure and operational controls. The internal audit had correctly identified the weaknesses, but the lack of clear ownership and urgency in the remediation process allowed the control failures to persist until the losses exceeded the bank's capital.

Key lesson: Lack of timely action of audit recommendations allowed risk to accumulate catastrophically.

Common Challenges in Remediation

Despite the importance of timely remediation, many organisations struggle to maintain momentum once the initial audit or assurance activity is completed. Several recurring challenges undermine progress and dilute the value of assurance.

Fragmented tools

Fragmented tools remain one of the most significant barriers. When findings are scattered across spreadsheets, shared drives, emails, and individual trackers, it becomes difficult to maintain a single source of truth. Version control issues emerge, status updates become unreliable, and leadership and the governing body loses visibility over real progress.

Unclear ownership

Unclear ownership further compounds the problem. Without a clearly assigned and accountable owner, actions fall into organisational grey zones. People leave and teams may assume another group is responsible, resulting in stalled remediation and follow-through.

Prioritisation

Weak prioritisation also leads to inefficiency. When all actions - minor process improvements and major control failures alike - are treated with equal urgency, resources are misallocated. High-risk issues that are complex to resolve require immediate attention will compete against low-impact recommendations, slowing down overall risk reduction.

Unrealistic deadlines

Timeframes are often set without considering workload, budget, or technical complexity. This leads to predictable delays. This creates a culture where extensions become expected, and due dates lose meaning, which in turn weakens governance oversight.

> ***A recent Audit Office of NSW report found that 40% of findings in local government are repeat findings.***

Closure governance

Insufficient evidence of closure is another widespread issue. Many actions are marked “complete” based on verbal confirmations or surface-level updates rather than genuine, documented proof that the control weakness has been addressed. This creates a false sense of assurance and can mask deeper systemic problems.

Weak or no validation by internal audit or an independent function exacerbates the issue. Without objective confirmation that remediation has occurred and is effective, organisations risk a false sense of assurance.

Inadequate monitoring & reporting

Inadequate reporting and escalation mechanisms hinder actionable oversight. Audit committees and senior executives often receive outdated or overly complex reports that don't highlight critical overdue issues or trends. Without formal escalation pathways for overdue or high-risk items, accountability breaks down and issues and risks persist far longer than they should.

These themes are also echoed in government audit office insights and professional internal audit guidance, which consistently emphasise the need for disciplined follow-up and documentation.

So What? Collectively, these challenges lead to a backlog of open findings, recurring issues in successive audits, and diminished confidence in the organisation's control environment. Overcoming them requires not only better tools, but a shift towards disciplined ownership, risk-based prioritisation, transparent reporting, and independent verification.

Carillion (2018)

Carillion's collapse triggered parliamentary and auditor scrutiny. Parliamentary and National Audit Office (NAO) reports noted that internal audit and external oversight failed to challenge key risks aggressively, with audit recommendations not sufficiently being acted upon and critical governance weaknesses ignored.

The strategic risk, cash flow and accounting issues culminated in the company's collapse.

Key lesson: Weak follow-up of audit and governance findings, combined with lack of escalation and fatal flaws in an organisation's control structure contributed to systemic failures.

Narrow focus & blind spots

Finally and most importantly, not all critical findings originate from internal audit reports.

Many organisations make the mistake of tracking only internal audit findings, leaving other critical assurance insights unmanaged. This narrow scope creates blind spots.

Major failures around the world demonstrate that unaddressed recommendations from penetration tests, vulnerability scans, engineering inspections, and other assurance reviews can be just as catastrophic. The Equifax data breach and the Genoa Morandi Bridge collapse are two stark reminders of what happens when non internal audit issues are identified - but not remediated.

Equifax (2017)

The 2017 Equifax data breach which exposed the personal information of 147 million people, was a direct result of a failure to fix a known vulnerability.

Equifax received an alert from US-CERT regarding a critical vulnerability in open-source software. It subsequently issued instructions to over 400 employees to patch the vulnerability within 48 hours. However, the company failed to alert the specific staff member responsible for the vulnerable system. To make things worse, Equifax "didn't check to make sure employees followed through on the patching process". This failure of management oversight meant the company failed to discover the unpatched vulnerability for over four months.

Key lesson: This case study highlights the importance of tracking and accelerating high-severity remediation and ensuring vulnerability management recommendations are implemented and evidenced.

The Genoa Morandi Bridge Collapse (Italy, 2018)

The catastrophic collapse of the Morandi Bridge in Genoa, Italy, on August 14, 2018, which killed 43 people, represents a profound failure to action critical engineering assurance. Months prior to the collapse, in February 2018, expert engineering reports quantified severe structural degradation. Despite critical, quantifiable assurance data, the management of the highway company and the supervising ministry failed to implement any critical mitigating actions. Options such as limiting traffic, diverting heavy trucks, reducing the roadway from two lanes to one, or simply reducing vehicle speeds were never considered necessary.

Key lesson: Failure to consider expert recommendation and deferred maintenance in critical infrastructure does not simply delay costs; it creates an unbudgeted, accumulating liability that eventually guarantees total system failure.

The Equifax breach and the Genoa Morandi Bridge collapse reinforce that catastrophic failures often come from risks identified outside internal audit. In both cases, clear early warnings existed i.e. technical vulnerability alerts in Equifax's environment and engineering deterioration reports in Genoa, yet these findings sat outside traditional remediation follow-up processes and were never effectively tracked, escalated, or closed.

So What? The case studies above reveal a simple truth; disasters rarely strike without warning. The signs were there - just scattered, siloed, or unseen. Broadening your issue and remediation tracking lens is not just better practice; it may be the only thing preventing the next headline.

A Framework for Remediation Governance

To overcome common remediation challenges and ensure assurance translates into real risk reduction, organisations need a structured, repeatable framework. This framework formalises accountability, improves visibility, and creates a clear path from findings to validated closure.

1. Capture & Centralise

All findings and recommendations, whether from internal audits, external audits, regulatory reviews, pen tests, vulnerability scans, or BCP exercises, should be consolidated into a single source-of-truth system. Centralisation eliminates fragmented spreadsheets and ad-hoc tracking, providing leadership and audit teams with a reliable, real-time view of open actions and progress.

2. Classify & Prioritise

Not all findings carry equal risk. Each recommendation should be assessed and prioritised based on risk, potential impact, and remediation cost. High-risk issues that threaten financial, operational, regulatory, or reputational outcomes receive immediate focus, while lower-risk actions are appropriately scheduled. Risk-based prioritisation ensures limited resources are deployed efficiently and effectively.

3. Assign Ownership

Each action must have a clearly accountable owner, typically a business unit head, IT manager, risk lead, or other responsible party. Clear ownership removes ambiguity, drives accountability, and ensures someone is actively responsible for progressing the action to completion.

4. Develop Remediation Plans

For every finding, organisations should create a detailed action plan outlining specific task, timelines, dependencies, resource requirements, and expected outcomes. Realistic planning helps prevent overdue actions, unrealistic deadlines, and stalled initiatives, while providing a roadmap for execution and oversight.

5. Define Evidence Requirements

Closure should never rely solely on verbal assurances. Organisations must specify what constitutes acceptable evidence of remediation. This could include test results, system screenshots, configuration changes, certificates, updated policies, or documented approvals. Clear evidence standards reduce ambiguity and strengthen confidence in closure.

6. Validation & Closure

Once evidence is collected, an independent review, typically by internal audit, should validate that the remediation is effective and sustainable before marking it formally closed. This step prevents “paper closures,” mitigates repeat findings, and reinforces governance integrity.

7. Escalation Rules

Formal escalation protocols should be established to manage overdue or high-risk items. For example, actions overdue by 90 days or those with unmet critical risk criteria should be escalated to senior management or the audit committee. Escalation ensures visibility of emerging risks and drives timely corrective action.

8. Continuous Monitoring

Remediation is not a one-off exercise. Organisations should track key metrics, refresh risk ratings, and maintain living dashboards to provide ongoing transparency and oversight. Continuous monitoring enables leadership to detect trends, evaluate effectiveness, and make informed decisions on resource allocation and risk prioritisation.

So What? By applying this structured framework, organisations move from reactive, fragmented tracking to proactive, transparent, and accountable remediation governance. Findings from audits, pen tests, and other assurance reviews become actionable intelligence, providing boards, audit committees, and executives with confidence that risks are being systematically addressed and that assurance truly drives organisational improvement.

Driving Action Through Technology

Effective remediation requires more than process discipline, it requires tools that enable transparency, accountability, and timely action.

Modern remediation tracking technology like InConsult's GuardianERM platform, and specifically its Audit Desk module, are designed to support organisations in converting audit and assurance findings into verified, actionable improvements. They help boards, audit committees, and executives monitor progress, identify bottlenecks, and ensure that risks are actively managed.

Key features of a robust platform include:

- ✓ **Unified Repository of Findings and Actions:** All internal audit, external audit, regulatory, cyber, and technical findings are consolidated into a single, centralised system, creating a reliable single source of truth. This eliminates fragmented spreadsheets and email trails, ensuring a complete and reliable view of open actions.
- ✓ **Role-Based Workflows:** Platforms allow for clearly defined roles - owners, actioners and validators - so responsibilities are transparent, and accountability is embedded into the workflow.
- ✓ **Evidence Upload and Versioning:** Action owners can attach supporting documentation – test results, screenshots, approvals, or configuration changes – directly to findings. Versioning ensures that historical records are preserved, providing a clear audit trail.
- ✓ **Audit Trail of Actions and Communications:** Every update, or modification is recorded automatically. This creates transparency, facilitates independent verification, and demonstrates compliance to regulators and auditors.
- ✓ **Metrics and Dashboarding Capabilities:** KPI tracking, dashboards, and reports allow leadership to quickly understand overdue actions, risk exposure, repeat findings, and remediation velocity. Boards and audit committees gain actionable insights at a glance.
- ✓ **Notifications, Reminders, and Escalation Workflows:** Automated alerts and reminders keep action owners and validators on track, while escalation rules ensure overdue or high-risk items reach the appropriate level of leadership.

So What? By using dedicated remediation software, organisations significantly reduce reliance on spreadsheets and manual tracking methods. This not only increases operational efficiency, but also improves governance transparency, provides a robust audit trail, and ensures that no finding is overlooked or delayed. In essence, technology acts as the backbone of effective remediation, transforming fragmented assurance processes into a coordinated, accountable, and auditable system.

The Remediation Lifecycle at a Glance

The remediation process follows a clear, repeatable lifecycle that ensures audit and assurance findings are captured, assigned, actioned, and independently verified. The diagram below illustrates the four core stages essential for strong remediation governance:

1. Data Collection

Findings from internal audit, external audit, penetration tests, vulnerability scans, and other assurance activities are gathered and prepared for entry into a central tracking system.

2. Centralised Tracking System

All findings are logged into a single remediation tracker, creating a consistent source of truth for ownership, deadlines, risk ratings, and status updates. This eliminates fragmented spreadsheets and enhances visibility across the organisation.

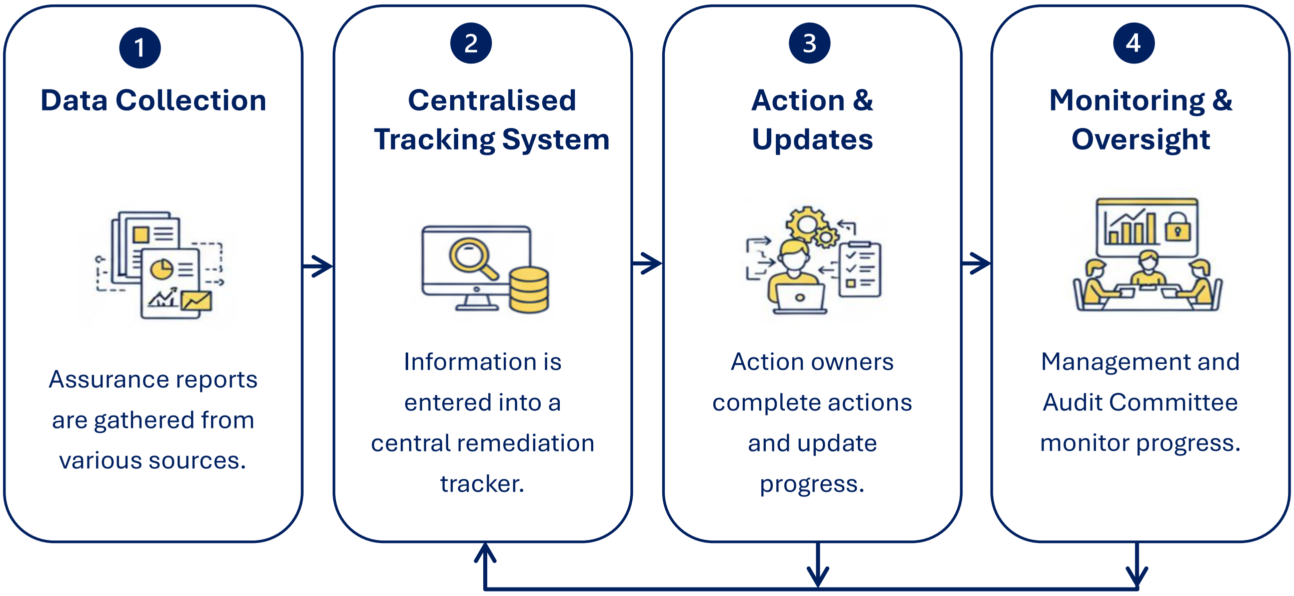
3. Action & Update

Action owners implement remediation activities, record progress, and upload evidence directly into the system. Frequent reminders ensure issues are acted on, not forgotten.

4. Monitoring & Oversight

Senior management and the Audit Committee monitor progress through dashboards and reports. Internal audit (or another independent function) validates completed actions before they are formally closed.

Together, these stages form a closed-loop process that transforms assurance findings into meaningful risk reduction and strengthens organisational resilience.



Assurance reports are gathered from various sources.

Information is entered into a central remediation tracker.

Action owners complete actions and update progress.

Management and Audit Committee monitor progress.

Metrics & KPIs: Measuring Performance

To ensure that remediation efforts are effective and accountable, organisations need to track and report meaningful metrics. Metrics provide a clear line of sight from audit and assurance findings to action completion, enabling boards, audit committees, and executives to monitor risk reduction and control improvement over time.

Key performance indicators (KPIs) that organisations should consider include:

- **Number of Open Recommendations by Severity:** Categorising open findings as Critical, High, Medium, or Low helps prioritise management attention and ensures resources are focused on the highest-impact issues.
- **Median Time to Close by Severity:** Tracking how long actions take to reach closure, segmented by risk level, identifies bottlenecks and highlights whether remediation timelines are realistic and being met.
- **Percentage of Closed Recommendations Validated by Internal Audit:** Demonstrates that closure is not just reported but independently verified, reinforcing governance integrity and providing assurance that risks have been effectively addressed.
- **Number of Repeat Findings Over Time:** Monitoring recurring issues—same or similar control failures—helps organisations identify systemic weaknesses, evaluate remediation effectiveness, and improve risk culture.
- **Overdue Items by Age Bands:** Segmenting overdue actions into intervals (e.g., 30-, 60-, 90-day) provides clarity on ageing backlogs, triggers escalation, and ensures that delayed items are addressed before they escalate into material risk.
- **Backlog Trend Analysis:** Year-over-year or quarter-over-quarter trends in open actions reveal whether remediation processes are improving, stagnating, or declining, enabling strategic adjustments to resourcing, prioritisation, and oversight.

These metrics are most effective when fed into a live, visually intuitive Audit Committee dashboard, providing a consolidated view of performance and highlighting systemic issues, trends, and areas requiring escalation. By monitoring these KPIs consistently, organisations can ensure that audit and assurance findings are not only resolved but translated into lasting operational and control improvements.

In essence, metrics transform remediation from a reactive exercise into a proactive governance tool, enabling leadership to make informed decisions, allocate resources efficiently, and demonstrate accountability to regulators, auditors, and stakeholders.

Why Independent Validation Matters

Validation by internal audit (or another independent assurance provider) is essential. It ensures closure isn't just a checkbox exercise and confirms that the risk is genuinely mitigated.

Without independent validation, there's a risk of "paper closures" - management signs off on remediation that never fully materialises. Internal audit validation preserves the objectivity of assurance, helps detect root-cause issues (e.g., control design flaws), and provides the audit committee with final comfort that risks are being addressed effectively.

Pattern of Unimplemented ANAO Recommendations (2024)

The Australian public sector provides more evidence of a recurring, structural failure to effectively implement the findings of the Australian National Audit Office (ANAO).

Reviews of implementation success reveal that agencies often engage in "implementation theatre," misrepresenting actual remediation. ANAO reviews found that 2 departments relied on insufficient or inadequate supporting evidence to close a significant number of recommendations.

Key lesson: The recurring pattern of recommendations being "closed" without adequate supporting evidence moves the issue beyond administrative delay into a category of deliberate non-compliance or fraud.

The IIA's International Professional Practices Framework (IPPF) requires a formal follow-up process, and governance standards argue strongly for audit committee oversight of remediation.

Roadmap for Implementation

Implementing an effective remediation framework requires a structured, phased approach that balances immediate impact with sustainable, enterprise-wide adoption. The roadmap below outlines three key phases, designed to deliver quick wins, build organisational capability, and embed a culture of continuous improvement.

1 LAUNCH	2 EXPAND & EMBED	3 SUSTAIN & IMPROVE
▪ Pilot remediation tracker in a key area	▪ Roll out system enterprise-wide	▪ Validate actions via internal audit
▪ Define evidence standards for closure	▪ Train owners, actioners, auditors	▪ Conduct regular trend reviews
▪ Socialise audit committee dashboard	▪ Embed KPIs into management reporting	▪ Develop remediation maturity model
▪ Assign remediation champion	▪ Establish escalation workflows	▪ Integrate performance into risk strategy

Phase 1: Launch (0 - 3 Months)

The first phase focuses on rapidly demonstrating value and generating momentum. By starting small, organisations can refine processes, build confidence, and showcase tangible results. Some of the key activities include:

- ✓ **Pilot a Remediation Tracker:** Select a key area such as internal audit or cybersecurity. Piloting allows teams to test workflows, refine evidence requirements, and identify system gaps before enterprise-wide rollout.
- ✓ **Define Standard Evidence Requirements for Closure:** Establish clear expectations for documentation of closure, such as test results, approvals, configuration changes, confirmation emails or meeting minutes. Standardising evidence reduces ambiguity and strengthens validation.
- ✓ **Socialise Reporting Dashboard for Audit Committees:** Even at pilot stage, provide leadership with visibility into open actions, progress, and overdue items. Early dashboards build confidence and reinforce accountability.
- ✓ **Assign a Remediation Tracker "Champion":** Designate an accountable owner who oversees the pilot, coordinates with actioners and validators, and drives completion. This role ensures ownership and visibility from day one.

Phase 2: Expand & Embed (3 - 6 Months)

Once the pilot demonstrates value, the next phase focuses on enterprise-wide adoption and capability building. Activities here include:

- ✓ **Roll Out the Remediation System Across the Organisation:** Extend the tracker to all business units, audit types, and assurance sources, ensuring a consistent, centralised approach.
- ✓ **Train Owners, Actioners, and Auditors:** Equip all participants with clear guidance on workflows, evidence standards, and system usage to embed accountability and operational consistency.
- ✓ **Embed Remediation KPIs into Audit Committee Reporting:** Introduce metrics such as open actions by severity, median closure times, repeat findings, and validation percentages. This ensures leadership oversight and risk-informed decision-making.
- ✓ **Develop Escalation Criteria and Workflows:** Define thresholds and escalation paths for overdue or high-risk items, ensuring timely action and continuous executive awareness.

Phase 3: Sustain & Improve (6 - 12 Months)

The final phase focuses on optimising performance, embedding governance, and driving continuous improvement:

- ✓ **Perform Internal Audit Validations and Refine Processes:** Validate that actions are genuinely resolved, learn from pilot and scaling experiences, and refine workflows and evidence requirements.
- ✓ **Establish Regular Trend Reviews:** Monitor metrics such as backlog reduction, repeat findings, and overdue items to identify systemic issues and emerging risks.
- ✓ **Build a Remediation Maturity Model:** Assess organisational capabilities, set performance benchmarks, and define pathways to higher maturity levels over time.
- ✓ **Incorporate Remediation Performance into Risk and Audit Strategy:** Use insights from tracked actions and metrics to inform broader risk management decisions, audit planning, and resource allocation.

Implementing effective remediation governance is not a complex transformation - it is a disciplined journey built on clear priorities, structured processes, and steadily increasing maturity. By starting small, scaling deliberately, and embedding continuous improvement, organisations can rapidly turn fragmented follow-up processes into a high-performing governance capability.

Conclusion

In many organisations, assurance reports are a treasure trove of insight – but insight alone is not enough. Too often, findings are acknowledged but not acted upon with the discipline, structure, and the transparency needed to meaningfully reduce risk. As a result, long-standing vulnerabilities remain embedded in business processes, control environments deteriorate over time, and repeat findings continue to frustrate executives and audit committees alike.

Without disciplined, evidence-backed follow-through, critical vulnerabilities and control gaps persist, often unnoticed until they are exploited or lead to failure.

By committing to a structured remediation framework, supported by a centralised remediation tracking system and independent validation, organisations can finally close the assurance loop. This shift transforms assurance from a retrospective diagnostic exercise into an engine of continuous improvement, one that strengthens controls, enhances resilience, and supports regulatory confidence. It ensures that every finding, regardless of type severity, receives appropriate action, ownership, and evidence before closure.

Most importantly, strong remediation governance demonstrates to Boards, audit committees, insurers, and regulators that leadership is committed to identifying and reducing risk.

The path forward does not require a massive overhaul. It begins with a single, practical step: launch a pilot remediation tracker in one high-risk domain within the next 30 days. Use it to model behaviours, refine processes, and demonstrate tangible progress. Within three months, present your first set of remediation metrics - open actions, overdue items, evidence quality, and repeat finding, to your Audit and Risk Committee. This early momentum is powerful as it builds confidence, supports cultural change, and positions the organisation to scale remediation governance enterprise-wide.

With consistent leadership commitment and the right tools, remediation excellence becomes achievable, measurable, and sustainable—transforming assurance insights into meaningful organisational resilience.

By adopting a structured remediation framework, a robust tracking system, and independent validation by internal audit, organisations can close the loop on findings and transform risk intelligence into sustained control.

The organisations that thrive are those that don’t just find issues, they fix them. Now is the time to move from insight to action and embed a culture of accountability and closure that safeguards performance, reputation, and long-term resilience.

Definitions

Action / Remediation Action	A specific task or set of tasks assigned to a responsible person to implement a recommendation and correct or mitigate the identified issue.
Action Owner	The individual responsible for implementing the remediation action, providing updates, and producing evidence of completion. Usually, a manager within the business unit where the finding occurred.
Aged Action	A remediation action that has been open for an extended period (commonly >90 or >180 days). Aged actions are a key risk and audit committee concern.
Assurance Backlog	The accumulated volume of open, overdue, or aged audit and assurance actions requiring remediation. Large backlogs indicate governance weaknesses.
Assurance Lifecycle (Finding-to-Fix Cycle)	The end-to-end process that spans issue identification, recommendation development, action planning, implementation, monitoring, validation, and closure. Also referred to as the “last mile of assurance.”
Assurance Report	A formal report produced by internal audit, external audit, regulators, cybersecurity teams, risk assessors, or other assurance providers that identifies findings, control weaknesses, risks, and recommendations requiring action.
Business Continuity (BCP) Exercise	A test or simulation to evaluate the organisation’s ability to operate during and after a disruption. Findings often generate improvement actions.
Closed Action	An action marked as complete by the business action owner but not yet independently validated by internal audit unless the organisation's policy allows self-closure.
Due Date	The target date by which an action must be completed. Typically based on risk severity, regulatory expectations, and business resource capacity.
Evidence of Completion	Documentation or artifacts demonstrating the action has been fully implemented (e.g., updated procedures, system screenshots, approvals, logs, configuration changes).
Finding (Issue)	A gap, weakness, non-compliance, vulnerability, or error identified through an assurance activity that requires remediation. Findings may be categorised by severity (e.g., Critical, High, Medium, Low).

Overdue Action	An action not completed by the agreed due date. Overdue actions often indicate resource issues, unrealistic deadlines, or poor remediation discipline.
Penetration Test (Pen Test)	A controlled cybersecurity assessment that simulates real-world attacks to identify vulnerabilities in systems, networks, or applications. Results feed into remediation actions.
Recommendation	A suggested action or remediation step made by an assurance provider to address the underlying cause of a finding, improve controls, or reduce risk.
Remediation Governance	The structures, controls, workflows, policies, and oversight mechanisms used to ensure audit actions are tracked, completed, and validated effectively.
Repeat Finding	A previously closed issue that re-emerges in a later audit due to inadequate remediation, poor validation, or insufficient evidence. Repeat findings signal weak governance.
Root Cause Analysis (RCA)	A structured method used to identify the fundamental cause(s) of an incident, failure, or audit finding. Effective RCA improves action relevance and prevents recurrence.
Three Lines Model	A governance model where operational management (Line 1), risk/compliance functions (Line 2), and internal audit (Line 3) have defined roles in risk and control oversight. Internal audit provides independent assurance and validation.
Validated Closure	The final stage of an action's lifecycle, where internal audit confirms that the action has been completed and adequately addresses the root cause. This is the gold standard of closure.
Validation (Internal Audit Validation)	An independent review performed by internal audit to confirm that a closed action is genuinely resolved, effective, and sustainable to prevent "paper closures."
Vulnerability Scan	An automated scan that identifies software, system, or network vulnerabilities. Often conducted regularly and linked to remediation workflows.

References & Further Reading

Reserve Bank of Australia (1995). *Implications of the Barings collapse for bank supervisors*. Reserve Bank of Australia Bulletin.

Apache Software Foundation (2017). *Media alert: Equifax data breach – Failure to install patches*.

United States Congress (2017). *An examination of the Equifax cybersecurity breach: Hearing before the House Committee on Energy and Commerce*.

Security Week (2017). *Equifax confirms Apache Struts flaw used in hack*.

Dark Reading (2014). *Target breach traced to HVAC contractor credential theft*.

Booth, R. (2018). *Key findings from MPs' report into Carillion collapse. The Guardian*.

The Institute of Internal Auditors (2018). *The Carillion failure: Misunderstood risks and constrained auditors*. The IIA Global.

International Organisation of Supreme Audit Institutions (INTOSAI) (2019). *ISSAI 3000 Performance Audit Standard*.

The Guardian (2019). *What caused the Genoa bridge collapse – and the end of an Italian national myth?*

Australian National Audit Office (ANAO) (2024). *Implementation of Parliamentary Committee and Auditor-General Recommendations — Department of Finance*

About InConsult

For 25 years, InConsult has been a trusted partner to boards, executives, audit committees, across public and private sector organisations seeking to strengthen governance, risk, and assurance capability. Based in Sydney and serving clients across Australia and internationally, InConsult brings deep expertise in internal audit, risk management, resilience, fraud & corruption prevention, cybersecurity, ESG, and governance advisory.

Through hundreds of internal audits, assurance reviews, risk assessments, and regulatory-aligned evaluations, InConsult has developed a practical understanding of the challenges organisations face- not only in identifying risks and control breakdowns, but in closing the loop by ensuring actions are implemented, validated, and sustained.

GuardianERM: Assurance Technology That Delivers Control

InConsult develops and delivers GuardianERM, an enterprise-grade Governance, Risk, and Compliance software platform designed to simplify and digitise risk, audit, and assurance processes. GuardianERM enables organisations to consolidate risk intelligence, optimise workflows, and enhance accountability across the three lines of defence.

Audit Desk: Purpose-Built for Audit & Assurance Action Tracking

At the centre of GuardianERM's assurance capability is Audit Desk - a dedicated module that streamlines the management of findings, recommendations, and remediation plans from:

- ✓ Internal audits
- ✓ External audits
- ✓ Compliance reviews
- ✓ Regulatory and tripartite reviews
- ✓ Penetration tests
- ✓ Vulnerability scans
- ✓ Incident investigations & root cause analyses
- ✓ Business continuity exercises
- ✓ Compliance and assurance reviews

Audit Desk provides a single source of truth for recording findings, assigning owners, tracking progress, and capturing evidence. With built-in escalation, automated reminders, reporting dashboards, and internal audit validation workflows. Audit Desk helps organisations reduce aged items, minimise repeat findings, and improve overall governance maturity.

InConsult's combination of practical audit experience and fit-for-purpose technology ensures that organisations not only identify risks - but manage and resolve them with discipline, transparency, and accountability.

GuardianERM

InConsult
risk advisory | audit | assurance

InConsult Pty Ltd
Level 35, One International Towers
Barangaroo Avenue, Sydney 2000

T: +61 2 9241 1344

www.inconsult.com.au
www.guardainerm.com

Notices

This ebook is provided for general informational and educational purposes only. It is not intended to constitute professional advice, guidance, or consulting services, nor should it be relied upon as a substitute for specific advice tailored to an organisation's circumstances. While every effort has been made to ensure the accuracy and relevance of the information contained herein, InConsult make no representations or warranties, express or implied, regarding the completeness, accuracy, or applicability of the content. In accordance with InConsult's AI Policy, AI tools were utilised to support the research, imagery, and development of this ebook. This process was guided by extensive human oversight and industry experience, with every reference rigorously validated against credible sources to ensure the highest standards of accuracy.

InConsult accept no responsibility for any loss, damage, or consequences arising from the use of, or reliance on, the information in this document. Organisations should seek appropriate professional advice before making decisions or implementing any of the practices described. All trademarks, names, or logos referenced in this ebook remain the property of their respective owners