Amstelveen

Building Risk-Based Internal Audit Plans: From Coverage to Prioritisation



Introduction

Organisations continue to face increasing regulatory expectations, growing risk complexity and ongoing pressure on Internal Audit capability and capacity. At the same time, Boards and Audit Committees expect assurance that is aligned to organisational priorities and focused on the risks, decisions and activities that have the greatest potential impact on organisational outcomes.

The IIA Global Internal Audit Standards (GIAS) reinforce this expectation. Internal Audit plans must be based on a documented assessment of the organisation's strategies, objectives and risks. This represents a shift away from plans driven by historical coverage or fixed audit cycles, towards a more deliberate and risk-informed approach to assurance planning.

For many organisations, the challenge is no longer whether the Internal Audit plan should be risk-based. The greater challenge is ensuring assurance priorities continue to evolve alongside organisational priorities. The greatest risk in Internal Audit planning is not missing a risk. It is failing to adapt assurance effort to changing strategic objectives, transformation activity, emerging risks and stakeholder expectations.

What should influence a risk-based Internal Audit Plan?

Risk-based Internal Audit planning is not about achieving coverage. It is about making deliberate prioritisation decisions.

Risk registers provide an important starting point but they are only one input into the planning process. Effective plans are informed by a broader set of factors, including strategic objectives, transformation initiatives, regulatory developments, emerging technologies such as AI, cyber threats, operational resilience programs, service provider dependencies, prior audit outcomes, incidents and stakeholder perspectives. No single input should determine audit priorities. Effective planning requires Internal Audit to bring together multiple sources of information and make informed prioritisation decisions based on organisational context and risk.



An environment scan helps Internal Audit understand how external pressures, market developments, regulatory change, major transformation programs, AI adoption and cyber security developments may change assurance priorities. These factors can introduce new risks or change the relative importance of existing risks.

Stakeholder engagement provides context that is often unavailable through documented information alone. Discussions with executives, business leaders and risk owners help Internal Audit understand how risks are being managed in practice, test whether documented risk assessments remain current and identify issues that may not yet be reflected in risk registers or planning documentation.

Prioritising Assurance

A risk-based Internal Audit plan is ultimately an exercise in prioritisation.

In practice, developing a risk-based plan involves making deliberate decisions about where assurance effort will be directed. Factors such as risk exposure, strategic significance, regulatory obligations, organisational change, previous assurance activity and available capability should all be considered when determining audit priorities.

Importantly, prioritisation also means deciding what will not be audited. Every review included in the plan comes at the expense of a review not performed. Internal Audit functions operate within finite resource and capability constraints. A plan that attempts to cover everything risks spreading effort too thinly and reducing the quality or relevance of assurance provided.

The strongest plans provide a clear rationale for why reviews have been included, why others have been deferred and how the overall plan supports organisational objectives. This transparency is important for management and Audit Committees, particularly where trade-offs have been made.

Making deliberate prioritisation decisions

Included	Deferred	Not prioritised
• High risk • Strategic importance • Regulatory obligations	• Lower risk • Resource constraints • Existing assurance	• Managed elsewhere • Duplication of assurance • Low value

Key Considerations

The objective is not to maximise coverage. It is to direct finite assurance effort towards the risks, decisions and activities that have the greatest potential impact on organisational outcomes.

Challenging and Refining the Plan

Audit Committee engagement should be more than formal endorsement of the plan. Every audit plan reflects choices:

> Mature Audit Committees focus not only on what has been included but also on what has been excluded and why.

Presenting the proposed Internal Audit plan provides an opportunity to challenge whether the right areas have been prioritised, whether the plan reflects current organisational risks and whether Internal Audit has the capability required to deliver the proposed work.

Every Internal Audit plan reflects a series of prioritisation decisions. Audit Committees should understand not only what has been included but also what has been excluded, deferred or addressed through alternative assurance mechanisms.

This provides transparency over the trade-offs that underpin the plan and enables more informed challenge and oversight.

Maintaining a risk-based plan therefore requires ongoing reassessment to ensure assurance priorities continue to reflect the current operating environment.

Questions Audit Committees should ask

1. What has changed since the plan was last approved?
2. What emerging risks, technologies or transformation activities may require future assurance attention?
3. Which risks or initiatives are not currently covered?
4. What assurance is already being provided by other functions?
5. Does Internal Audit have the capability required to review higher-risk or specialist areas?
6. What has been deferred, and why?

Keeping the plan relevant

Risk-based planning should not be viewed as an annual exercise.

Many organisations operate with rolling multi-year Internal Audit plans. While this provides useful visibility over future assurance activity, the plan should be reviewed periodically to ensure it remains aligned with organisational priorities and risk exposures.

Strategic priorities evolve, transformation programs progress and regulatory expectations continue to develop. Emerging technologies, cyber threats, operational resilience initiatives and large-scale transformation programs can quickly alter assurance priorities and should trigger reassessment of the plan. A plan that was appropriate twelve months ago may no longer reflect where assurance should be focused. Maintaining a risk-based plan therefore requires ongoing reassessment and not simply an annual refresh.

Key Considerations

The greatest risk in Internal Audit planning is not missing a risk. It is failing to adapt assurance effort to changing strategic objectives, transformation activity, emerging risks and stakeholder expectations.

Conclusion

The GIAS has strengthened expectations that Internal Audit planning should be grounded in organisational objectives, strategies and risks. A successful Internal Audit plan should not be measured by the number of areas reviewed, but by whether assurance effort is directed to the organisation's most significant risks and priorities.

Ultimately, the effectiveness of an Internal Audit plan should not be measured by the breadth of coverage it achieves. It should be measured by whether assurance effort is directed towards the risks, decisions and changes that matter most to organisational success.

A risk-based Internal Audit plan is not an exercise in coverage. It is an exercise in prioritisation.

Our Authors



Katherina Sau CA CIA
Director

Katherina is a risk and assurance professional with over 10 years of experience supporting internal audit and risk management functions to execute assurance plans and enhance risk maturity across organisations. She has also supported the development of multi-year internal audit plans for her clients, with her portfolio spanning public and private sectors, including Financial Services, Infrastructure, Education, and Health.



Jessica Cheung
Senior Manager

Jessica is a risk and assurance professional with 10 years of experience across technology risk, operational risk and controls assurance. She has supported financial services, telecommunications and fintech organisations through assurance reviews, control assessments and risk uplift initiatives. Jessica has experience establishing assurance programs, assessing control effectiveness and supporting governance and Board reporting. Jessica also has experience designing SOCI TSRMP frameworks within regulated organisations.



Meet Vyas
Consultant

Meet is a risk consultant with experience supporting internal audit, technology risk and process improvement activities across financial services. He applies analytical and technical skills to strengthen controls, improve system-enabled processes and uplift risk frameworks. His work includes controls testing, data integrity reviews and technology risk assessments across cybersecurity, general IT controls and data management.

View all services and case studies

Amstelveen

Email info@amstelveen.com

Website www.amstelveen.com

LinkedIn www.linkedin.com/company/amstelveen-pty-ltd

Amstelveen equips organisations to identify, assess and mitigate their most significant risks. Our risk, compliance and technology professionals support clients to improve the governance of their organisations. We provide specialist support to the largest public and private organisations in Australia and New Zealand. This publication contains general information only. We accept no duty of care nor liability for reliance on the information within it. To obtain information specific to your circumstances, please contact us at info@amstelveen.com.