European Confederation of
Institutes of
Internal Auditing

INTERNAL AUDIT RELIANCE STRATEGY IN THE BANKING INDUSTRY

ECIIA Banking Committee

June 2026

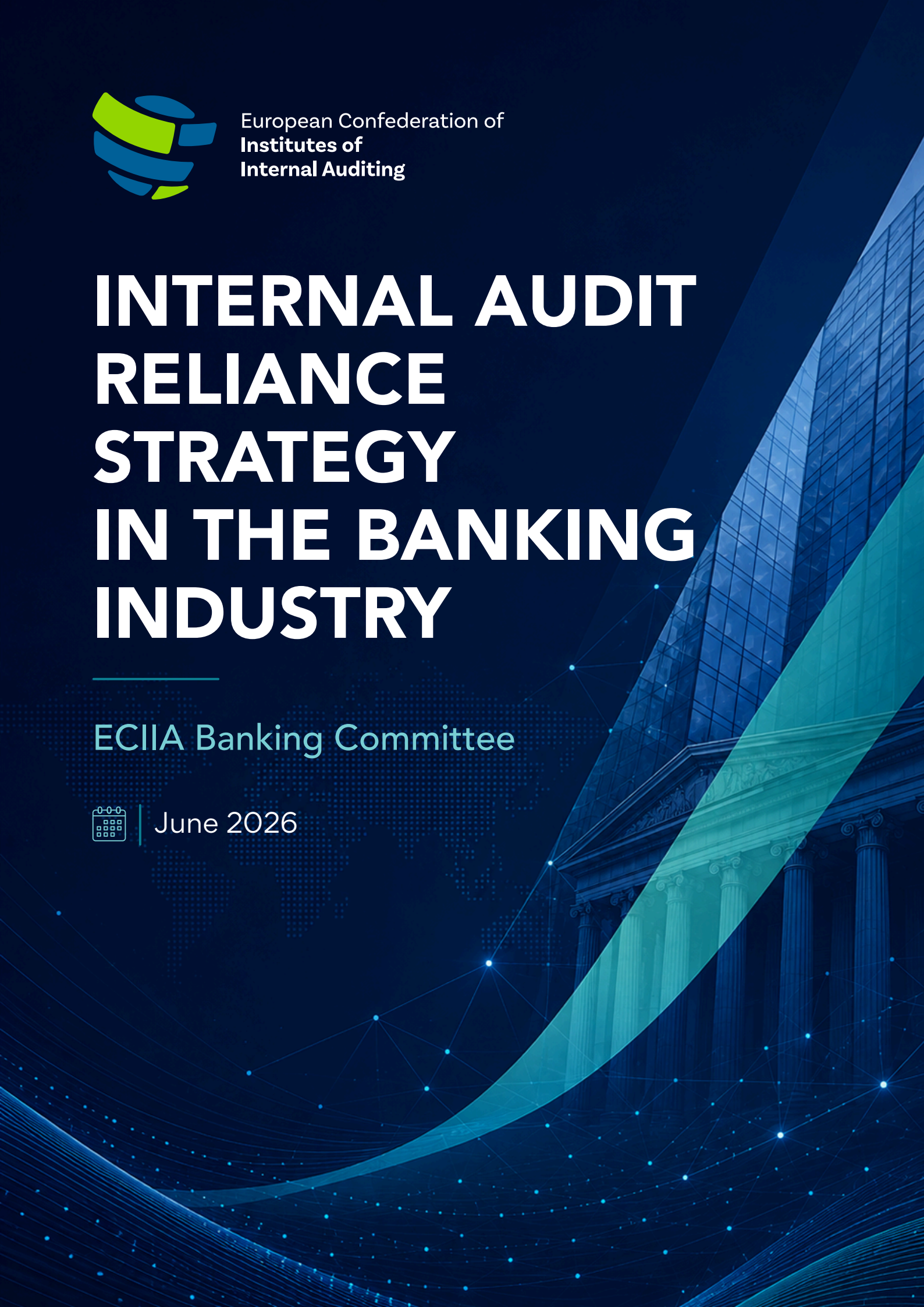


TABLE OF CONTENTS

INTRODUCTION

Reliance as a strategic question for Internal Audit in banks

Recent changes to the internal control landscape for European financial institutions have made reliance a more relevant and pressing question in the context of Internal Audit (IA) functions. There is a growing expectation that IA functions further develop their views on whether reliance should contribute to their assurance strategy and how this could be achieved.

This paper aims to provide inputs to inform this strategic decision, by gaining a better understanding of the prerequisites, constraints, benefits and opportunities of a reliance strategy. It also proposes an approach to make that decision and build a roadmap to implementation. In addition, it outlines limits of reliance and provides guidelines to validate the assumptions and conditions.

> **In auditing, "reliance" refers to the extent to which an auditor relies on the work of others, such as external auditors, specialists, or other lines of defence, when forming an audit opinion.**

The framework governing auditing practices plays a crucial role in shaping how audit strategy on reliance on other internal controls functions or assurance providers apply. This framework consists of various regulations, guidelines and standards, which are established by regulatory bodies and professional organisations.

The framework governing auditing practices plays a crucial role in shaping how audit strategy on reliance on other internal controls functions or assurance providers apply. This framework consists of various regulations, guidelines and standards, which are established by regulatory bodies and professional organisations.

EBA GUIDELINES

The EBA Guidelines on internal governance[1], currently under review, are highly relevant for reliance strategies as they require clear documentation of the roles and responsibilities of key risk and control functions, along with a detailed mapping and separation of duties.

IIA STANDARDS

The Global Internal Audit Standards issued by the Institute of Internal Auditors (IIA)[2] emphasise the importance of collaboration among assurance providers to improve the effectiveness of governance, risk management and control processes.

UK & US PRACTICE

In the UK, reliance is allowed by the Chartered Institute of Internal Auditors providing that IA assesses the maturity and effectiveness of the 1st and 2nd lines, validates the quality of their work and documents the rationale for reliance. In practice, reliance is acceptable only when the second line has robust, independent, and well-documented processes. In the US, reliance is permitted, as the condition that IA can justify and support its approach as regulators may scrutinize reliance decisions.

The European Central Bank (ECB), through its Single Supervisory Mechanism (SSM), expects significant institutions to have an effective IA function that operates independently, and objectively. ECB encourages coordination among internal control functions to ensure comprehensive oversight. Nevertheless, it has not produced any comprehensive guidelines on reliance. Therefore, implementing any reliance strategy between Audit and other assurance providers is the full responsibility of the Bank. It remains fundamentally bank-specific and depends on the maturity, robustness, and governance of each institution's risk and control framework.

Consequently, a reliance model cannot be standardised across the industry and must be adapted to each institution's context. It must also respect the full alignment of internal control around the Three lines of Defence framework and must preserve the strict independence and integrity of the Audit function.

Expectations of senior management and governance bodies have also been redefined, pushing for a more pertinent control framework and forward-looking, risk based, proactive audit function rather than retrospective reporting alone.

They emphasise the importance of a coordinated approach to governance, risk and control, advocating a combined assurance view that aligns with organisation's objectives and risk appetite.

We will examine first what reliance means in the specific context of the banking industry. Then, we will discuss the main steps for implementing a reliance strategy before drawing some decision factors for its implementation.

Our focus will be on the IA reliance strategy in the banking industry, excluding other types of reliance, such as the reliance of external audit on IA.

01

WHAT RELIANCE MEANS FOR FINANCIAL INSTITUTIONS

a Impact on audit processes

While IIA Global Internal Audit standards provide several examples of coordination with other assurance and advisory service providers, they are less descriptive regarding reliance and how it could impact the audit processes.

For the purpose of this paper, we focused on three potential impacts of reliance:

Audit coverage

IA may adjust audit frequency by leveraging results of the controls from other assurance functions. For instance, when the second-line reviews demonstrate a strong control framework, the residual risk of an auditable entity is reduced, allowing it to be audited less frequently. This approach is typically applied to areas with lower inherent risk or where robust second-line assurance effectively mitigates risk. The outcome is fewer entities covered for audit-cycle reasons and a more efficient, risk-based audit plan.

Audit testing

In an audit, IA may decide not to test some controls if another assurance function has already tested them and IA has assessed the quality of that work, determining that reliance can be placed. Institutions may consider limiting this approach to controls mitigating low or moderate risks, or to operational effectiveness testing only (i.e. auditors would still perform design assessment). This approach to reliance reduces the volume of testing required as part of audits.

Issue validation

IA may rely on other assurance providers for issue validation and the closure of audit recommendations, except for the most sensitive issues. However, this reliance is only appropriate if the 2nd line's process for approving implementation is demonstrably objective, independent, and robust. Recommendations should only be considered closed when there is clear evidence of a permanent change in operations. IA should also periodically review the 2nd line's closure process to ensure these standards are consistently met.

b Identification of assurance providers

The assurance mapping exercise can help to identify the various internal and external assurance providers and clarify their roles and the scope of their work, as prescribed by Standard 9.5 and Standard 6.1.

External assurance providers to consider for reliance include external auditors (statutory auditors), mutualised audits[3], and providers offering certification under the ISAE 3402/SSAE 16 standard for outsourced services[4] or ISO certification organisations[5]. For outsourced services, contracts generally include an audit clause. Execution of these audit rights may be undertaken by IA, the first line of defence, or independent external auditors. In practice, reliance is also placed on the outsourcing provider's own risk and control framework.

Internal assurance providers may include first and second line of defence, as well as previous audits. Additionally, the growing reliance on automated controls and data analytics creates new opportunities to enhance the assurance framework.

While this paper focuses on reliance from an IA standpoint, it is important to note that reliance can be mutual. For instance, the third line of defence may depend on the results of the second line, while the second line may rely on the findings of the third line to feed its oversight responsibilities. Regulators and Supervisors may also rely on the work of audit or request an audit.

As an example, in many banks, remediation packages for ECB findings are reviewed by the audit function before being sent to the Regulator. This interdependence highlights that assurance in financial institutions is not one-directional but collaborative across lines of defence.

02

PREREQUISITE, OBLIGATIONS AND ENABLERS FOR A RELIANCE STRATEGY

Implementing a reliance strategy is not merely a procedural adjustment. It involves several prerequisites regarding the selection of assurance providers and introduces dependencies that must be carefully managed. Several organisational enablers also support its effective use. A sound reliance approach must include strong checks and balances. Without clear rules, it can weaken the third line's independence or place undue trust in assurance providers with uneven maturity. Reliance should therefore be clearly framed, well documented, regularly reassessed, and supported by solid governance safeguards.

a Selection of assurance providers

The first prerequisite of a reliance strategy is the selection of the assurance providers, as not all assurance providers may be suitable for reliance. Standard 9.5 of the Global Internal Audit Standards outlines the essential criteria that must be considered when determining the appropriateness of reliance, and the Reliance Assessment Tool released by the IIA provides guidance on this process.

Four criteria must be considered to perform this assessment:

Independence and objectivity assessed through reporting relationships, identification and disclosure of conflict of interests. Assurance providers on which IA places reliance should be sufficiently independent within the organisation to provide objective assurance, consistent with the standards required for IA.

Competency including the relevance and validity of professional experience, qualification and certifications of the teams involved in the assurance process.

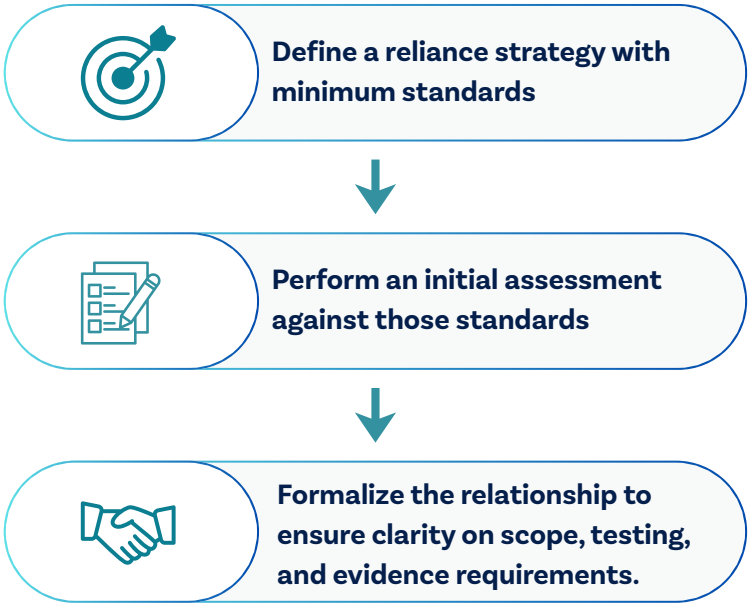
Elements of practices assessed based on methodology and due professional care for risk assessment, planning and performance of assurance engagements.

Communication of results to an appropriate level of management, ensuring that assurance providers relied upon meet equivalent quality standards and lead to consistent conclusions.

In addition, reliance on the 2nd line is only appropriate where the 2nd line's activities are sufficiently mature, well-resourced, and comprehensive. IA should not compensate for deficiencies in the 2nd line's activities. If such deficiencies are identified, they should be escalated to governance bodies and reliance should not be applied.

b Validation and documentation of prerequisites

As provided by IIA Global Internal Audit Standards: "*If the internal audit function intends to rely upon the work of another assurance provider on an ongoing or long-term basis, the parties should document the agreed-upon relationship and specifications for the assurance to be provided, and the testing and evidence required to support the assurance.*" According to the IIA's Reliance Assessment tool, a formal agreement must be in before proceeding further with an evaluation to determine reliability. A structured approach could be: first, define a reliance strategy with minimum standards; next, perform an initial assessment against those standards; and finally, formalize the relationship to ensure clarity on scope, testing, and evidence requirements.



> After evaluating the work of another assurance provider, the chief audit executive may determine that the internal audit function cannot rely upon the work. Internal auditors may either retest the work and gather additional information or independently perform assurance services.

This process may raise questions about the approach taken to assess the reliability of an internal assurance provider. For instance, organisations will have to consider whether they should perform specific audits for this purpose or leverage their existing audits. The frequency of these assessments is also a consideration: determining an appropriate schedule is essential for maintaining confidence in the reliance strategy. If we consider the three lines set up, this might require the third line of defence to conduct more audits on the second line. It is critical to validate and document that these prerequisites are met as part of the reliance strategy.

It is also imperative that any reliance arrangements are reported to the Audit Committee. This ensures that the committee is aware of the assurance strategy and can provide oversight and guidance on the strategy's effectiveness.

C Enablers of Reliance

While many European financial institutions have established a shared risk taxonomy across internal control functions, there remains significant diversity in risk assessment methodologies, risk universes, and supporting tools. This diversity can hinder the effectiveness of reliance strategies. Therefore, strengthening harmonization and building a robust, common control framework is essential to maximize the benefits of reliance.

Though not prerequisites, several enablers[6] are essential components to facilitate the implementation of reliance across internal assurance providers:

Common approach to Risk/Audit Universe:

ensuring consistency in the way risk and audit universes are designed avoids painful reconciliation efforts. For instance, reliance may be more challenging if the second line of defence adopts a process-based risk universe, while IA has a purely legal entity – organisational view-based audit universe.

Common risk assessment methodology:

sharing the same risk scoring methodology, or at least the same risk scoring scale, and a common calendar are also enablers ensuring that all teams operate with the same understanding of risk and severity assessment (which does not imply that teams will have the same opinion on the risk score) at the same time.

Consistency of control plans and multi-year coverage:

Ensuring that control review plans are consistent, and that multi-year risk coverage is comprehensive and aligned with the bank's risk profile. This helps avoid duplication, identify gaps, and support an integrated assurance approach.

Common issue remediation framework:

developing a harmonised framework for managing action plans in response to findings and issues raised by all lines of defence and following up (through the same tool and process) is important to ensure that the IA team can rely on the assurance provider to remedy the identified weaknesses.

Common tools:

such tools, such as modern GRC tools, can serve as facilitators in organising reliance by sharing data across lines of defence such as risk assessment, control plans, control results, action plans, risk and control indicators or operational incidents.

Common governance:

involving the main assurance providers to ensure coordinated reporting to the Audit Committee and to the executive management.

d Impact of New Technologies and AI on Reliance Strategies

The rise of IT, data analytics, and artificial intelligence (AI) is profoundly reshaping internal control and audit functions in financial institutions. While AI-powered controls and advanced analytics can enhance efficiency and risk coverage, they also introduce new challenges, such as ensuring the reliability and auditability of automated processes, and upskilling teams to assess AI-driven outputs.

As these technologies continue to develop, Internal Audit must regularly review and document its reliance strategies, ensuring clear criteria, robust governance, and continuous assessment of their impact on the three lines of defence.

Organisations applying reliance need to establish clear criteria for reliance, validating and documenting compliance with these prerequisites, and leveraging enablers. This approach helps improve IA and encourages better accountability across assurance functions.

However, the Head of IA remains ultimately accountable for the assessments performed by assurance providers on which he or she has decided to rely and remains responsible for the reliance strategy. This should be regularly reviewed—adjusting it if risks increase or audit results raise concerns.

03

IMPLEMENTING A RELIANCE APPROACH: A STRATEGIC DECISION

Before implementing a reliance strategy, it is critical to conduct a detailed cost/benefit analysis. The complexity, duration, and rigor required by reliance may, in some cases, outweigh the anticipated benefits.

It also carries inherent risks if not properly framed: it can weaken independent judgement, place trust in assurance work that does not meet audit standards, or lead to under-scoping and missed emerging risks. These vulnerabilities make it necessary to validate reliance assumptions regularly, reinforce documentation, and establish clear escalation mechanisms.

A thorough evaluation ensures that the approach is tailored to the institution's specific context and objectives.

BENEFITS	COSTS
Improved efficiency and relevance	Upgrades to assurance functions and risk management framework
Reduced control workload/fatigue	Assessment of assurance providers
Enhanced risk coverage	Additional audits and selection costs
Better resource utilisation	Production of an assurance map
Meaningful insights for the audit committee	Increased documentation and reporting
	Potentially increased audit risk

BENEFITS OF A RELIANCE APPROACH

Improved efficiency and relevance:

Leveraging outcomes and insights from other assurance functions enables IA to streamline its processes, focus resources and coverage on areas with higher risk leading to more efficient and more relevant audit processes.

Reduced control workload/fatigue:

A reliance strategy can significantly reduce control workload and fatigue by alleviating the burden on business units, allowing them to concentrate on their core activities. Additionally, this approach fosters collaboration among assurance providers, eliminating duplication of efforts and promoting a more cohesive assurance environment.

Enhanced risk coverage:

Integrating various assurance functions enables organisations to gain a more comprehensive understanding of risks, thereby improving overall risk coverage.

Better resource utilisation:

By focusing on the most significant risks, organisations can allocate resources more effectively, ensuring they are directed towards areas requiring the most attention.

Meaningful insights for the audit committee:

A well-implemented reliance strategy can provide the audit committee with more relevant and actionable insights, enhancing its oversight capabilities.

COSTS OF A RELIANCE APPROACH

Upgrades to assurance functions and risk management framework:

Implementing reliance may necessitate enhancements to existing assurance functions and risk management frameworks in order to meet the established quality requirements and implement enablers.

Assessment of assurance providers:

IA will need to evaluate whether reliance can be placed on other assurance providers, considering factors such as independence and governance, maturity, methodology/framework, and overall quality. This assessment requires additional time, expertise, and resources.

Additional audits and selection costs:

Organisations may need to focus the audit function more on the evaluation of the effectiveness of assurance-providing functions, thereby increasing the overall workload. However, this additional effort may be offset by benefits such as improved efficiency, better resource utilisation, and enhanced coordination among assurance providers.

Production of an assurance map:

Developing a more detailed assurance map is essential for visualising the roles and interactions of various assurance providers and requires significant effort and resources.

Increased documentation and reporting:

The reliance strategy will necessitate extra documentation and reporting to validate compliance with prerequisites and communicate effectively with all stakeholders.

Potentially, increased audit risk:

By relying on the work of other assurance providers, the Internal Audit function may face higher audit risk. Mitigating measures include assessing these providers and enforcing the reliance enablers outlined in previous sections.

04

THE ROADMAP TO RELIANCE

Given the complexity of implementing a reliance approach, it is important to recognise that this is an ongoing and incremental process.

The following key steps should be considered when building a reliance roadmap:

1 COORDINATION

Establishing a shared methodology and framework is an essential requirement. It is also vital to establish clear lines of communication and collaboration among the various assurance functions. This ensures that all parties are aligned in their objectives and understand their roles.

IA and assurance providers should coordinate closely regarding their respective plans to avoid duplication of work, ensure that all risks are reviewed, and enable the IA team to build on the work of the assurance providers when launching an audit mission.

2 COLLABORATION

Fostering a culture of collaboration among the first, second and third lines of defence enhances the effectiveness of the internal control framework within the organisation. Regular meetings, joint risk assessment discussions and shared reporting can strengthen relationships and improve overall assurance quality.

3 PROGRESSIVE IMPLEMENTATION OF RELIANCE

If they choose to implement a reliance strategy, organisations should adopt a phased approach. This may involve starting with pilot programmes to allow for the gradual integration of reliance practices, followed by broader implementation as confidence in the approach grows.

4 CONTINUOUS EVALUATION

As the reliance strategy is rolled out, it is crucial to continuously evaluate its effectiveness and make necessary adjustments. IA needs to regularly assess the work quality of those on whom it relies. Feedback from assurance providers, business units and the audit committee can inform ongoing improvements to the reliance framework.

THE FUTURE OF RELIANCE

The concept of reliance will evolve.

The evolution of technologies is creating an environment where large data repositories are shared across lines of defence and tools based on data analytics and AI to provide early detection and faster investigation capabilities to all lines of defence.

This transformation will reshape the control framework landscape in financial institutions, shifting and blurring the frontiers between lines of defence in some areas, and ultimately changing the approach to reliance.

For instance, one might question how IA would operate and consider reliance in an organisation where the first line has automated a large part of its controls and where second-level control teams have implemented a fully data-driven and AI-powered assurance framework.

CONCLUSION

Internal control functions across financial institutions are becoming more specialized, more interconnected, and more collaborative.

This evolution naturally raises the question of whether reliance practices can help internal audit go further in terms of efficiency, coverage, and insight. Yet the length, complexity, and level of discipline required by a reliance strategy must be carefully weighed against its potential benefits.

Reliance is not simply the reuse of prior work. It involves a comprehensive understanding of the roles and interactions of various assurance functions, as well as a continuous assessment of the quality of the assurance they produce.

If not properly framed, reliance can weaken independent judgement, expose IA to work that does not meet audit standards, or create blind spots and miss emerging risks. These risks call for strong governance, enhanced documentation, regular validation of reliance assumptions, and robust escalation mechanisms.

Any reliance strategy must therefore be designed in a way that fully preserves third-line independence. The chief audit executive remains accountable and independent for the conclusions reached. It requires time and constant assessment by third line of defence of the quality of the other assurance providers.

A clearer regulatory framework on the conditions for applying reliance within European banking groups would support more consistent, safe, and effective practices. In the meantime, institutions considering reliance should adopt a cautious, structured, and context-specific approach, anchored in strong governance and aligned with the fundamental principles of the Three Lines of Defence.

REFERENCES & NOTES

01 European Banking Authority (EBA), “Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05),” 2 July 2021, scheduled to be reviewed by Q3 2026 according to the EBA Work Programme in 2026

02 The Institute of Internal Auditors (IIA) Standard 9.5 – Coordination and Reliance: “The chief audit executive must coordinate with internal and external providers of assurance services” and Standard 6.1 Internal Audit Mandate requires that the CAE must coordinate with other internal and external assurance providers to gain an understanding of each other’s roles and responsibilities to help the board and senior management determine the scope and types of internal audit services.

03 Mutualized audits organized by the Collaborative Cloud Audit Group (CCAG) for big tech cloud services (e.g., Microsoft Azure or AWS) or those organized by the French “Comité inter-inspections générales” (CIIG) on shared providers.

04 International assurance standard that describes Service Organization Control (SOC) engagements, which provides assurance to an organization's customer that the service organisation has adequate internal controls.

05 **ISO certification organisations** - Independent organisation which verifies that a company's internal systems, like manufacturing processes or service procedures, meet internationally recognized standards for quality and consistency.

06 The enablers identified in section 2 echo the recommendations of the Institut Français de l'Audit et du Contrôle Interne paper on the efficiency of internal control (IFACI, 2019).

ABOUT ECIIA

The European Voice of Internal Audit

The European Confederation of Institutes of Internal Auditing (ECIIA) is the representative body of internal audit profession at European level, brigning together 35 National Institutes and representing more than 58,000 internal auditors across Europe.

Through advocacy, thought leadership, research and engagement with regulators and policymakers, ECIIA promotes strong corporate governance and effective internal audit across Europe.

By fostering collaboration among Institutes and professionals, ECIIA supports the development of internal audit as an independent, objective assurance and advisory function that creates value and strengthens trust in organisations.

ECIIA BANKING COMMITTEE

The ECIIA Banking Committee brings together Chief Audit Executives and senior internal audit professionals from European banks.

The Committee contributes to the development of the profession by sharing knowledge, addressing emerging risks and supporting the continuous improvement of internal audit in the banking sector.

It engages with regulators and supervisory authorities and serves as a consolidated voice of internal auditing in European banking.

Established as one of ECIIA's sectoral committees, the Banking Committee contributes to thought leadership, regulatory dialogue, and the advancement of internal audit practices within the European banking sector.

ECIIA

www.eciia.eu

info@eciia.eu

ECIIA - European Confederation of Institutes of Internal Auditing